Doc. No. 78-3335-02

Second-Generation Channel Interface Processor (CIP2) Installation and Configuration

Product Numbers: CX-CIP2-ECA1=, CX-CIP2-ECA2= , CX-CIP2-ECAP1=, CX-CIP2-PCA1=, CX-CIP2-PCA2=, CX-CIP2-U-ECA1=, CX-CIP2-U-ECA2=, CX-CIP2-U-ECAP1=, CX-CIP2-U-PCA1=, CX-CIP2-U-PCA2=, CAB-PCA-Y=, CAB-PCA-VA=, CAB-PCA-VB=

This document contains instructions for installing (or replacing) the second-generation Channel Interface Processor (CIP2) in the Cisco 7000 series routers and the Cisco 7500 series routers.

Important Note to Users The following Cisco Internetwork Operating System (Cisco IOS) releases support the CIP2: Cisco IOS Release 10.2(13), or later, Release 10.3(13), or later, Release 11.0(10), or later, or Release 11.1(5) or later.

Prior to these Cisco IOS releases being available, CIP2 is supported with a special microcode image. This microcode image is available through download from Cisco Connection Online (CCO), on diskettes shipped with the CIP2 when shipped separately from a system (as a spare), or is already in Flash memory on a preconfigured system. For instructions on placing CIP2 microcode in Flash memory, see the section “CIP2 Microcode” on page 37.

Once CIP2 microcode has been copied into Flash memory, a configuration command must be specified to instruct the Cisco IOS to use this microcode image instead of the microcode image bundled with your version of the Cisco IOS. For instructions on configuring the Cisco IOS to use a CIP2 microcode image from Flash memory, refer to the section “Configuring Microcode” on page 39.

For additional specific CIP2 software and hardware requirements, refer to the section “Software and Hardware Prerequisites” on page 13. For complete and detailed descriptions of CIP2-related interface and configuration commands, configuration options, and requirements, refer to the publications listed in the section “If You Need More Information” on page 2.

Document Contents

This document includes the following sections:

If You Need More Information

The Cisco Internetwork Operating System (Cisco IOS) software running your router contains extensive features and functionality. The effective use of many of many of these features is easier if you have more information at hand. For additional information on configuring and maintaining the Cisco 7000 series and Cisco 7500 series routers and CIP2, the following documentation resources are available to you:

- Cisco Connection Documentation, Enterprise Series CD-ROM

  This publication and additional Cisco Systems publications are available on a CD-ROM called Cisco Connection Documentation, Enterprise Series, which is Cisco's online library of product information. The CD-ROM is updated and shipped monthly, so it might be more up to date than printed documentation. To order Cisco Connection Documentation, Enterprise Series CD-ROM, contact a Cisco Sales or Customer Service representative.

- Refer to the following modular configuration, modular command reference, and support publications, as appropriate for your configuration:

  — *Configuration Fundamentals Configuration Guide*

  — *Configuration Fundamentals Command Reference*

  — *Security Configuration Guide*

  — *Security Command Reference*

  — *Wide-Area Networking Configuration Guide*

  — *Wide-Area Networking Command Reference*

  — *Network Protocols Configuration Guide, Part 1*

  — *Network Protocols Command Reference, Part 1*

  — *Network Protocols Configuration Guide, Part 2*

  — *Network Protocols Command Reference, Part 2*

  — *Network Protocols Configuration Guide, Part 3*

  - *Network Protocols Command Reference, Part 3*
  - *Bridging and IBM Networking Configuration Guide*
  - *Bridging and IBM Networking Command Reference*
  - *Configuration Builder Getting Started Guide*
  - *Troubleshooting Internetworking Systems*
  - *Debug Command Reference*
  - *System Error Messages*
  - *Cisco IOS Software Command Summary*
  - *Cisco Management Information Base (MIB) User Quick Reference*
- For hardware installation and maintenance information on the Cisco 7000 series and Cisco 7500 series routers, refer to the following publications:
  - *Cisco 7000 Hardware Installation and Maintenance*
  - *Cisco 7010 Hardware Installation and Maintenance*
  - *Cisco 7505 Hardware Installation and Maintenance*
  - *Cisco 7507 Hardware Installation and Maintenance*
  - *Cisco 7513 Hardware Installation and Maintenance*
- To view Cisco documentation or obtain information about documentation, refer to the Cisco Connection Documentation, Enterprise Series CD-ROM, to the section “Cisco Connection Online,” on page 46, or call Customer Service at 800 553-6387 or 408 526-7208. Customer Service hours are 5:00 a.m. to 6:00 p.m. Pacific time, Monday through Friday (excluding company holidays). You can also send e-mail to `cs-rep@cisco.com`. You can also refer to the *Cisco Information Packet* that shipped with your router.

What Is the CIP2

This section discusses channel attachment and the CIP2, its LED functions, and its memory and cable requirements.

Channel Attachment Overview

A mainframe channel (referred to as a *channel*) is an intelligent processor that manages the protocol on the communications media and controls the data transfer to and from the main central processing unit (CPU) storage. Devices called input/output processors (IOPs) communicate between the host CPU and the channel. One IOP controls multiple channels, and there is no relationship between the number of CPUs and the number of IOPs.

The channel relieves the mainframe CPU of direct communication with input/output (I/O) devices, which saves processing cycles and allows data processing and communications tasks to run concurrently. Channels use one or more channel paths as the links between mainframes and I/O devices. I/O devices are connected directly to control units, which provide the logical capabilities required to operate and control the I/O devices.

CIP2 Overview

The CIP2 provides up to two channel-attached interfaces for Cisco 7000 series and Cisco 7500 series routers, eliminating the need for a separate front-end processor.

The CIP2 interfaces are combinations of a bus and tag (also called an original equipment manufacturer's interface [OEMI] and a parallel I/O interface) adapter and an Enterprise Systems Connection (ESCON) adapter.

The bus and tag adapter is called the Parallel Channel Adapter (PCA), and the ESCON adapter is called the ESCON Channel Adapter (ECA). The PCA and ECA connect directly to the CIP2, and any combination of the two adapters can be used.

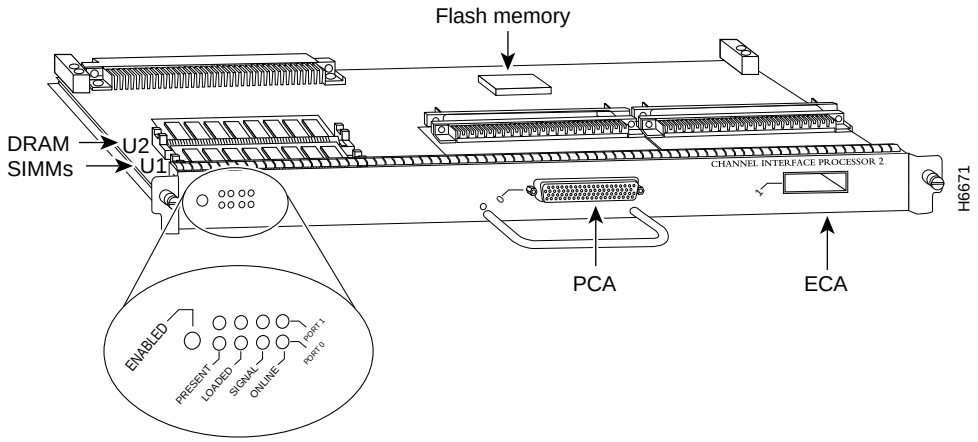
Note The ECA and PCA adapters can be upgraded or replaced (in the field) by a Cisco-certified maintenance provider *only*. The CIP2 supports online insertion and removal (OIR), which allows you to install or remove a CIP2 while the system is operating, without shutting down system power.

Caution To prevent system problems in Cisco 7000 series and Cisco 7500 series systems running Cisco IOS images earlier than Cisco IOS Release 11.1(5), CIP2 (second-generation) cards must not be installed in the same chassis system with CIP (first-generation) cards.

CIP2 Description

The CIP2 (see Figure 1) consists of a motherboard that is mounted on a metal carrier and one or two ECA and/or PCA interfaces. (The CIP2's reads *Channel Interface Processor 2*.) The ECA and PCA interfaces attach to the motherboard by means of a multipin connector located at the rear edge of the adapter. The CIP2 has two DRAM SIMMs (see Figure 1) and comes configured with 32 MB of DRAM as the minimum standard (default) memory configuration. The CIP2 also has a Flash memory device for storing the CIP2 microcode boot image. (See Figure 1.)

Figure 1 Channel Interface Processor, Horizontal Orientation



Note The ECA and PCA adapters can be upgraded or replaced (in the field) by a Cisco-certified maintenance provider *only.*

Caution To prevent damage, and to prevent insertion problems caused by misalignment of the adapters and motherboard, do not attempt to remove the adapters or motherboard from the carrier.

CIP2 Model Numbers

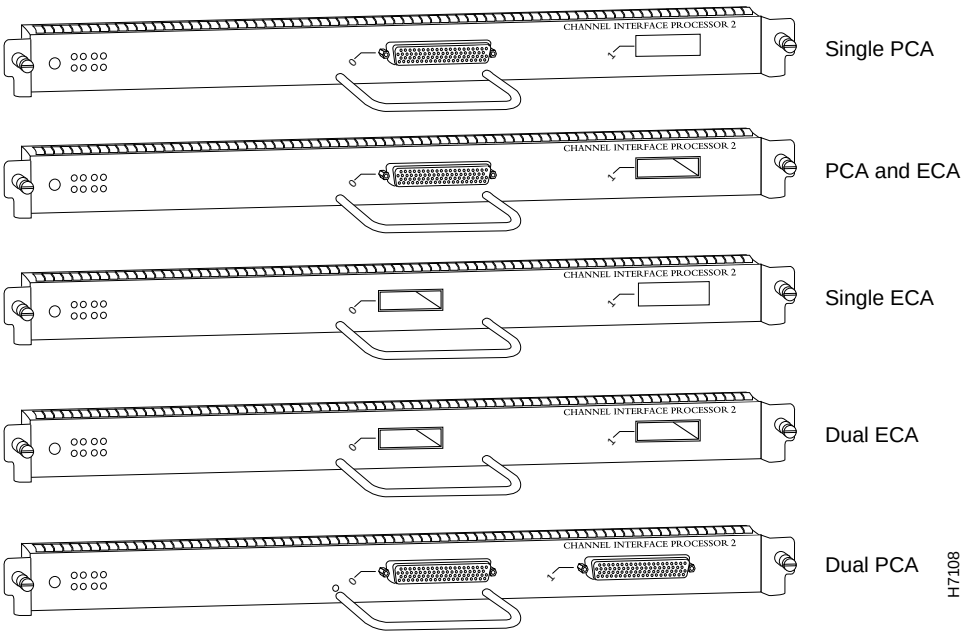
There are three CIP2 carrier types, which offer the following five interface adapter combinations:

- Single PCA on a PCA/ECA carrier (CX-CIP2-PCA1)
- Combination PCA and ECA (CX-CIP2-ECAP1)
- Single ECA on a dual ECA carrier (CX-CIP2-ECA1)
- Dual ECA on a dual ECA carrier (CX-CIP2-ECA2)
- Dual PCA on a dual PCA carrier (CX-CIP2-PCA2)

Add an equal sign (=) to the product number when you order interface processors as spares.

The ECA has a female, duplex connector, and the PCA has a female, DB-78 connector. Figure 2 shows the ECA and PCA interface combinations.

Figure 2 CIP2 Interface Adapter Combinations



CIP2 DRAM Configurations

Each CIP2 model is available in the following configurations of dynamic random-access memory (DRAM) single in-line memory modules (SIMMs):

- 32-MB DRAM—MEM-CIP-32M[1]
- 64-MB DRAM—MEM-CIP-64M(=)
- 128-MB DRAM—MEM-CIP-128M(=)

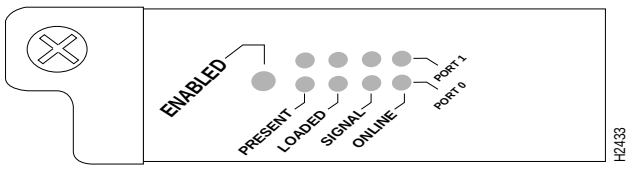
Note CIP2 DRAM can be upgraded in the field by Cisco-certified service personnel *only.*

1. 32 MB of DRAM is the default memory configuration for the CIP2.

CIP2 LED Indicators and Sequences

Following are the functions of the CIP2 LEDs. (See Figure 3.)

Figure 3 CIP2 LED Indicators



- Enabled—Indicates that the CIP2 has been enabled for operation by the system.
- Present—Indicates that the ECA or PCA adapter has been detected by the CIP2.
- Loaded—Indicates that the ECA or PCA adapter firmware has been completely loaded.
- Signal—For the ECA, this LED indicates that the Sync signal has been detected. For the PCA, this LED indicates that the Operational Out signal has been detected. Note that even though a system reset and selective reset both cause the operational out signal to drop, the signal LED will still be on during those sequences.
- Online—For the ECA, this LED indicates that an establish-logical-path request has been received from the channel. For the PCA, this LED indicates that the PCA is ready to establish connection to the host channel.

Following are the sequences for the CIP2 LED indicators. The enabled LED is not part of the following sequences. On cold boots, the following LED sequences apply:

	Present	Loaded	Signal	Online
Port 1	On	On	Off	Off
Port 0	Off	Off	Off	Off

	Present	Loaded	Signal	Online
Port 1	On	On	On	On
Port 0	On	On	Off	Off

	Present	Loaded	Signal	Online
Port 1	On	On	On	On
Port 0	On	On	On	On

The following LED sequence indicates that the CIP2 is waiting for commands from the RP (or RSP).

	Present	Loaded	Signal	Online
Port 1	Off	Off	Off	Off
Port 0	Off	Off	Off	Off

On warm boots, the LEDs flash briefly. On downloads, the following three LED sequences apply; the first indicates that the system is downloading volatile programmable logic device (VPLD) code:

	Present	Loaded	Signal	Online
Port 1	On	On	On	On
Port 0	On	On	On	Off

The following sequence indicates that the CIP2 is downloading microcode:

	Present	Loaded	Signal	Online
Port 1	Off	Off	Off	Off
Port 0	On	On	On	On

The following sequence indicates that the CIP2 is starting to execute the microcode:

	Present	Loaded	Signal	Online
Port 1	Off	Off	Off	Off
Port 0	Off	Off	Off	Off

ESCON and Bus and Tag Specifications

Table 1 lists the specifications for the ESCON and bus and tag interfaces.

Table 1 ESCON and Bus and Tag Specifications

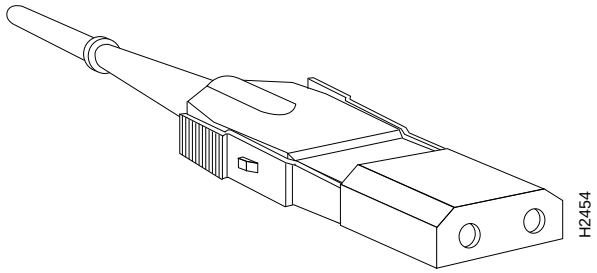
Characteristic	ESCON	Bus and Tag
Supported processor I/O architectures	ESA/390	System/370 370/Xa ESA/390
Bit transmission	Serial	Parallel
Maximum distance (for LED with ESCON)	1.9 miles (3.1 km) point-to-point 5.7 miles (9.2 km) with two ESCON Directors	400 ft (122 m)[1]
Channel data rate	Up to 17 MBps[2]	Up to 4.5 MBps
Signaling rate[3]	200 Mbps[4]	4.5 MBps
Cable types	Fiber-optic (62.5/125 micron multimode)	Copper bus and tag
Connection types	Dynamic[5]	Static
Number of addressable devices per channel	256 x 16 x 16 x 253[6]	256
Connectable control units per channel	Up to 59 (through a 9032 ESCON Director)	Up to 8
Connectable channels per adapter	Up to 59 (through a 9032 ESCON Director) Varies by control unit	1

1. The IBM 3044 C/D (host side/remote side) copper-to-fiber repeater can be used to extend this distance up to 1.2 miles (2 km).
2. MBps = megabytes per second.
3. For bus and tag, the signaling rate matches the channel data rate. For example, if you use a 3.0 MBps channel, the signaling rate is 3.0 MBps. The ESCON interface signals at a constant rate; the bus and tag interface signals at the data rate.
4. Mbps = megabits per second.
5. The CIP2 ESCON requires dynamic = NO with HCD.
6. Where 256 represents available unit addresses, 16 represents the number of partitions (LPARs), 16 represents the number of control unit images, and 253 represents the number of ESCON director paths. It is unlikely a system would have the resources to support the total number of available addresses.

ESCON Cable

The ECA interface uses 62.5/125 micrometer, multimode, fiber-optic cable with male duplex connectors at each end. (See Figure 4.) ESCON cables are not available from Cisco Systems. Refer to the ESCON specifications in Table 1, and contact your cable supplier or the vendor of your host CPU to order the correct ESCON cable.

Figure 4 ESCON Interface Duplex Connector for the ECA



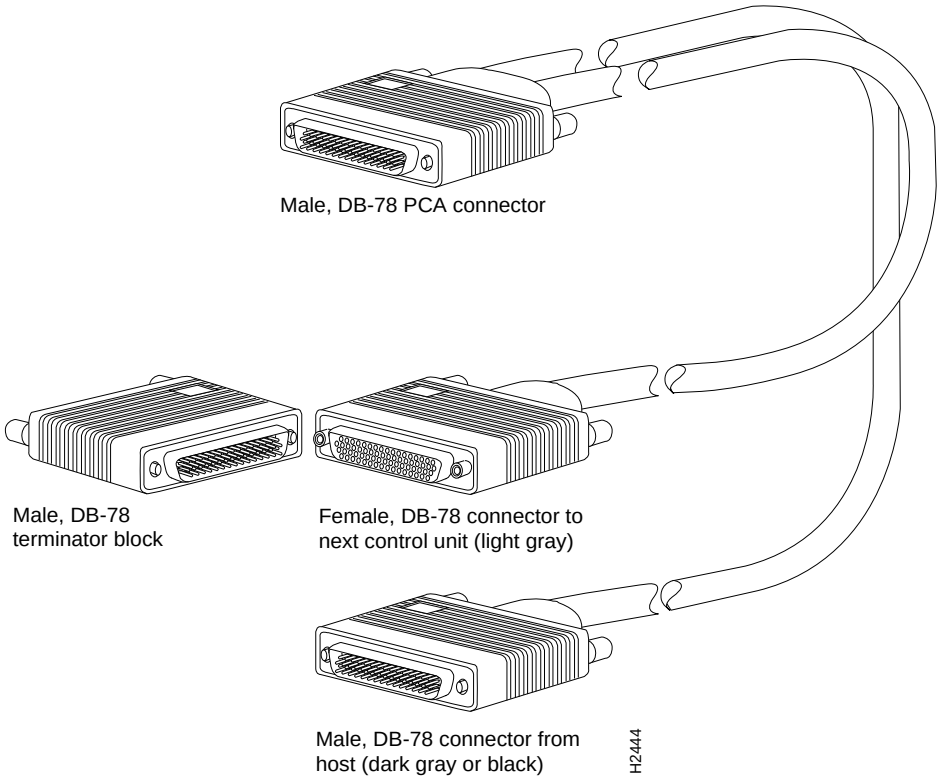
Bus and Tag Cables

Following are descriptions and illustrations of the bus and tag cables.

Y Cable

The bus and tag cable with three 78-pin connectors (shown in Figure 5) has a DB-78 male (PCA) connector on the CIP2 end, a DB-78 female connector on the next-control-unit end, and a DB-78 male connector on the from-host end.

Figure 5 PCA Bus and Tag Cable (CAB-PCA-Y)



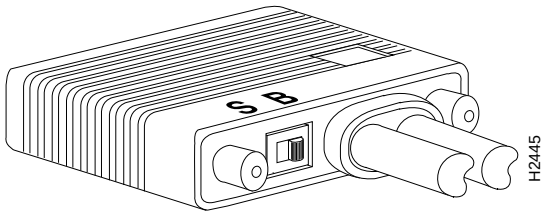
The model number is CAB-PCA-Y (referred to as the *Y cable*) The male connector might be labeled *IN* and is typically black, but can also be a dark gray. The female connector might be labeled *OUT* and is typically light gray. The female OUT cable is nearest to the select/bypass switch, which is discussed on the following page. (The IBM part number is 89F8392; however, this is subject to change.)

Caution The Y cable must connected directly to the PCA. Do not connect any other cables directly to the PCA.

Note the switch marked *S* (for select mode) and *B* (for bypass mode). The switch is located on the rear of the PCA connector. (See Figure 6.) The select/bypass switch is required to allow the cable to be separated from the PCA without "opening" the select-out loop.

Caution To prevent halting the system or negatively affecting the mainframe operating system, verify that the select/bypass switch is in bypass mode before you remove the PCA connector from the CIP2.

Figure 6 Select/Bypass Switch on the Rear of the PCA Connector (CAB-PCA-Y Bypass Shown)



In select mode the PCA is operational, and the select-out signal is passed in a loop to all control lines on the channel. All control units have a relay that shorts the incoming select-out signal to the outgoing select-out signal when power is not applied to the control unit. When power is applied, the relay is opened, and the signal is passed to the PCA.

Without the select/bypass switch in bypass mode, the channel would need to be taken offline before servicing or replacing a CIP2. If the selected address does not match, the select-out signal is passed to the next control unit. If the select-out signal gets all the way back to the channel, the control unit being addressed is not present.

Note In bypass mode, the incoming select-out signal is shorted to the outgoing select-out signal, bypassing the PCA and allowing other devices on the channel to function properly.

Caution Make sure you provide adequate strain relief for the heavy bus and tag cables that attach to the PCA, to prevent damaging the PCA connector on the CIP2 by unintentionally disconnecting the Y cable from the PCA connector.

VA and VB Cables

The two bus and tag cables with connector blocks have a DB-78 (male or female) connector on the CIP2 end and 48-pin type-A connector blocks on the bus and tag ends. (See Figure 7.) VA and VB cables are 56 inches (1.42 meters) in length.

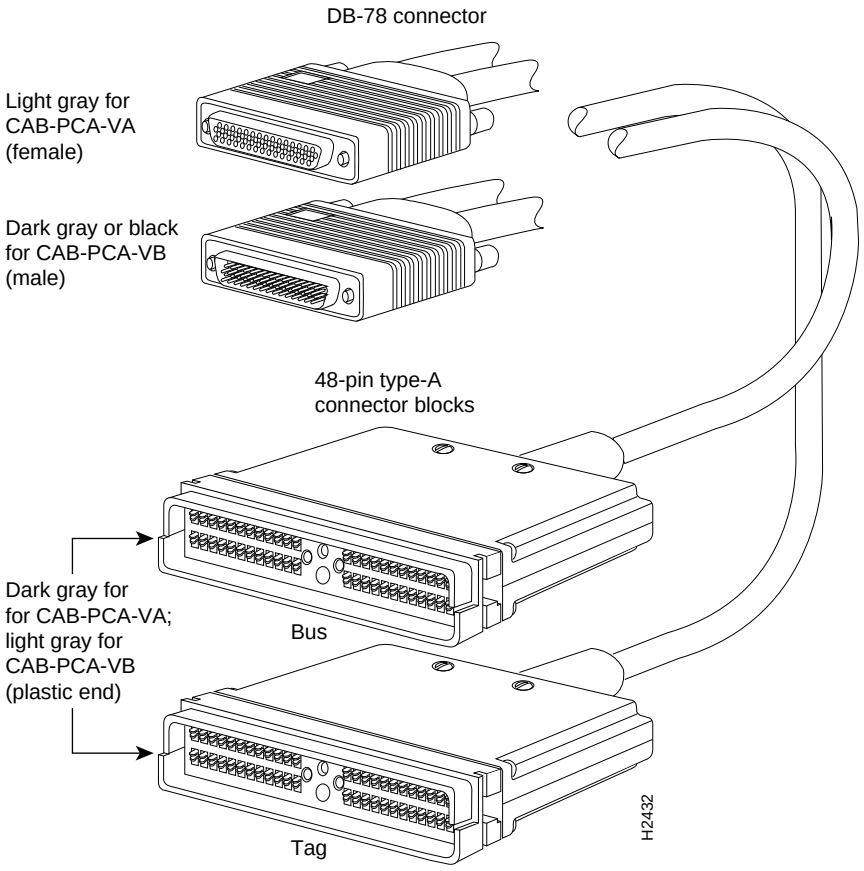
For the bus and tag cable that attaches between the host and the PCA, the model number is CAB-PCA-VA, and it is referred to as the *VA cable*. The female 78-pin connector might be labeled *IN* and is typically light gray. The cable labeled *P2* is bus, and the cable labeled *P3* is tag. Looking into the end of the female 78-pin connector (on the VA cable), with the wide part of the connector D-shell on top, the P2 (bus) cable is on the right, and the P3 (tag) cable is on the left. The plastic on the ends of the bus and tag connectors might be black or dark gray.

The IBM part number is 12G8058; however, this is subject to change. The VA cable ships with a terminator; the Cisco model number CAB-PCA-VA includes this terminator. The terminator and VA cable together have the IBM part number 12G7988; however, this is subject to change.

For the bus and tag cable that attaches between the next control unit and the PCA, the model number is CAB-PCA-VB, and it is referred to as the *VB cable*. The male 78-pin connector might be labeled *OUT* and is typically black or dark gray. The cable labeled *P2* is bus, and the cable labeled *P3* is tag. Looking into the end of the male 78-pin connector (on the VB cable), with the wide part of the connector D-shell on top, the P2 (bus) cable is on the left, and the P3 (tag) cable is on the right. The plastic on the ends of the bus and tag connectors might be light gray (as opposed to the black or dark gray plastic on the VA cable). The IBM part number is 12G7933; however, this is subject to change.

Caution To prevent potential system problems, do not connect the VB cable directly to the PCA. You must connect the Y cable to the PCA, then connect the VB cable to the Y cables as appropriate.

Figure 7 PCA Bus and Tag, VA and VB Cables



The Y cable always attaches to the PCA. The VA cable attaches between the male end of the Y cable and the host. The VB cable attaches between the female end of the Y cable and the next (or new) control unit. Do not connect the VB cable directly to the PCA. If the PCA is the last control unit, channel termination is required at the end of the Y cable that points away from the host. (See Figure 5.) For attachment instructions refer to the section “Attaching the CIP2 to the Channel” on page 30.

Caution To prevent damaging the PCA connector on the CIP2 by unintentionally disconnecting the Y cable from the PCA connector, provide adequate strain relief for the heavy bus and tag cables that attach to the PCA.

Installation Prerequisites

Before you install the CIP2, review the safety and electrostatic discharge (ESD)-prevention guidelines in this section to avoid injuring yourself or damaging the equipment. This section also provides a list of parts and tools you will need to perform the installation, and lists the software and microcode requirements.

Software and Hardware Prerequisites

You can determine the current version of software or microcode stored in Flash memory either by removing the processor module and checking the Flash device's label or by configuring the system to boot the system software from Flash memory, reloading the system, and using **show** commands to check the version that is loaded and running. Refer to the section "CIP2 Microcode," on page 37, for basic configuration information, and to the appropriate software documentation for complete configuration instructions and examples. If the displays indicate that the required system software and microcode is not available in your system, refer to the section "Cisco Connection Online," on page 46, for information about contacting a service representative for upgrade information.

Following are important software and hardware prerequisites concerning the CIP2:

- To operate with the CIP2, the Cisco 7000 series systems require Cisco IOS Release 10.2(13), or later, Release 10.3(13), or later, Release 11.0(10) or later, or Release 11.1(5) or later.
- To operate with the CIP2, the Cisco 7500 series systems require Cisco IOS Release 10.3(13), or later, Release 11.0(10), or later, or Release 11.1(5) or later.

Note Refer to Table 2, on page 14, for the specific Cisco IOS images.

- The CIP2 operates with the CxBus in the Cisco 7000 series routers with either of the following processor types:
  - Route Processor (RP) and Switch Processor (SP) (or Silicon Switch Processor [SSP]) combination.
  - 7000 Series Route Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI) combination.
- The CIP2 operates with the CyBus in the Cisco 7500 series systems, which use the Route Switch Processor (RSP).

Caution To prevent system problems in Cisco 7000 series and Cisco 7500 series systems, running Cisco IOS images earlier than Cisco IOS Release 11.1(5), CIP2 (second-generation) cards must not be installed in the same chassis system with CIP (first-generation) cards.

Table 2 (on the following page) lists the specific Cisco IOS software release images that are compatible with the CIP2.

Table 2 Cisco IOS Release Image Names

Cisco IOS Release	Image Names[1]
Release 10.2	gs7-k2 gs7-p2-m
Release 10.3	gs7-k2-mz gs7-p2-mz rsp-k2-mz rsp-p2-mz
Release 11.0	gs7-k2-mz gs7-p2-mz gs7-ak2-mz rsp-k2-mz rsp-p2-mz rsp-ak2-mz
Release 11.1	gs7-p-m gs7-aj gs7-ajv gs7-j gs7-jv gs7-pv gs7-s gs7-p rsp-p-m rsp-aj rsp-ajv rsp-j rsp-jv rsp-pv rsp-p

1. The Cisco IOS Release 10.2, Release 10.3, and Release 11.0 image names that specifically contain a "2" are compatible with the CIP2. All Cisco IOS Release 11.1 image names are compatible with the CIP2.

The **show version** and **show hardware** commands display the current hardware configuration of the router, including the system software version that is currently loaded and running. The **show microcode** command lists the bundled microcode (target hardware) version for each processor type. The CIP (and now CIP2) microcode is no longer bundled in Cisco IOS 11.1 and later, so the show microcode command lists the default microcode which should be used with this Cisco IOS version. The **show controller cbus** command shows the microcode version you are running. (For complete descriptions of configuration commands, refer to the publications listed in the section "If You Need More Information" on page 2.)

You can determine the current version of software or microcode stored in Flash memory either by removing the processor module and checking the Flash device label or by using the **show controller cbus** command and checking the *EPROM version* number in the output. Refer to the section "CIP2 Microcode," on page 37, for basic configuration information, and to the appropriate software documentation for complete configuration instructions and examples, listed in the section "If You Need More Information" on page 2.

If the displays indicate that the required system software and microcode is not available in your system, refer to the section "Cisco Connection Online," on page 46, or contact a service representative for upgrade information.

Safety Guidelines

This section lists safety guidelines you should follow when working with any equipment that connects to electrical power or telephone wiring.

Electrical Equipment

Follow these basic guidelines when working with any electrical equipment:

- Before beginning any procedures requiring access to the chassis interior, locate the emergency power-off switch for the room in which you are working.
- Disconnect all power and external cables before moving a chassis.
- Do not work alone when potentially hazardous conditions exist.
- Never assume that power has been disconnected from a circuit; always check.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Carefully examine your work area for possible hazards such as moist floors, ungrounded power extension cables, and missing safety grounds.

Telephone Wiring

Use the following guidelines when working with any equipment that is connected to telephone wiring or to other network cabling:

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.

Preventing Electrostatic Discharge Damage

ESD damage, which can occur when electronic cards or components are improperly handled, results in complete or intermittent failures. Each processor module contains a printed circuit card that is fixed in a metal carrier. Electromagnetic interference (EMI) shielding, connectors, and a handle are integral components of the carrier. Although the metal carrier helps to protect the board from ESD, use an ESD-preventive wrist or ankle strap whenever you handle any electronic system component.

Following are guidelines for preventing ESD damage:

- Always use an ESD-preventive wrist or ankle strap and ensure that it makes good skin contact.
- When you work at the interface processor end of the chassis, connect the equipment end of the strap to a captive installation screw on an installed interface processor, or to any unpainted chassis surface.
- When you install a processor module, use the ejector levers to properly seat the bus connectors in the backplane, then tighten both captive installation screws. These screws prevent accidental removal, provide proper grounding for the system, and help to ensure that the bus connectors are seated in the backplane.

- Handle processor modules by the carrier handles and carrier edges only; never touch the board or any connector pins.
- When you remove a processor module, place it card side up on an antistatic surface or in a static shielding bag. Immediately place the module in a static shielding bag if you need to return it to the factory.
- Avoid contact between electronic equipment and clothing. Antistatic straps only protect the equipment from ESD voltages on the body; ESD voltages on clothing can still cause damage.

Caution For safety, periodically check the resistance value of the antistatic strap. The measurement should be between 1 and 10 megohms.

Online Insertion and Removal—An Overview

The OIR feature allows you to remove and replace interface processors while the system is operating; you do not need to notify the software or shut down the system power.

Note This section describes the mechanical functions of the system components and emphasizes the importance of following the correct procedures to avoid unnecessary board failures. This section is for background information only; specific procedures for the CIP2 are contained in the following sections.

Each interface processor contains a male connector with which it connects to the system backplane. Each card (male) connector comprises a set of tiered pins, in three lengths. The pins send specific signals to the system as they make contact with the backplane. The system assesses the signals it receives and the order in which it receives them to determine what event is occurring and what task it needs to perform, such as reinitializing new interfaces or shutting down removed ones.

For example, when inserting an interface processor, the longest pins make contact with the backplane first, and the shortest pins make contact last. The system recognizes the signals and the sequence in which it receives them. The system expects to receive signals from the individual pins in this logical sequence, and the ejector levers help to ensure that the pins mate in this sequence.

When you remove or insert an interface processor, the backplane pins send signals to notify the system, which then performs as follows:

1. Rapidly scans the backplane for configuration changes.
2. Initializes all newly inserted interface processors, noting any removed interfaces and placing them in the administratively shut down state.
3. Brings all previously configured interfaces on the interface processor back to the state they were in when they were removed. Any newly inserted interfaces are put in the administratively shut down state, as if they were present (but unconfigured) at boot time. If a similar interface processor type has been reinserted into a slot, its ports are configured and brought on line up to the port count of the original interface processor.

The system brings on line only interfaces that match the current configuration and were previously configured as up; all others require that you configure them with the **configure** command.

OIR functionality enables you to add, remove, or replace interface processors with the system on line, which provides a method that is seamless to end users on the network, maintains all routing information, and ensures session preservation.

Tools and Parts Required

You need the following tools and parts to install or replace a CIP2. If you need additional equipment, contact a customer service representative for ordering information.

- Number 2 Phillips or one-quarter-inch flat-blade screwdriver for the captive installation screws on the CIP2. (Although most interface processors use slotted screws, some interface processor carriers use Phillips screws.)
- A new CIP2 with one of the product numbers listed on page 1 or in the section "CIP2 Model Numbers" on page 5.
- The appropriate cables for your CIP2 type: bus and tag for a PCA (with terminal blocks or 78-pin connectors) and/or ESCON fiber with duplex connectors for an ECA.
- ESD-preventive wrist strap or other device for preventing ESD damage.
- Interface processor filler (MAS7K-BLANK) if you are removing a CIP2 and not installing a new CIP2 or other interface processor in the empty slot.

Microcode Overview

Microcode, also known as firmware, is a set of processor-specific software instructions that enables and manages the features and functions of a specific processor type. At system startup or reload, the system loads the microcode for each processor type present in the system.

The CIP2 microcode boot image resides in a Flash memory device on the CIP2 motherboard. The entire CIP2 microcode image is delivered on a Flash memory card, on floppy disks, or is available via download from CCO.

New microcode is released to enable new features, improve performance, or fix bugs in earlier versions. The Cisco 7000 series and Cisco 7500 series routers feature downloadable software and microcode for most upgrades. These features enable you to download new (upgraded) images remotely, store the images in router memory, and load the new images at system startup without having to physically access the router. You can store multiple versions for a specific processor type in Flash memory, and use configuration commands to specify which version the system should load at startup. All interfaces of the same type (for example, all CIP2s) use the same microcode image.

Caution To ensure proper operation of the CIP2, and to preclude system problems, you should use *only* the CIP2 microcode image that is recommended for the version of Cisco IOS you are running. By default, the CIP2 microcode is loaded from either the flash memory (if you have a 7000 and 7010 with a RP) or the Flash memory card in slot0. The default version can be found by entering the **show microcode** command.

Following is an example of the **show microcode** command output:

```
Router# show microcode
Microcode bundled in system

Card    Microcode    Target Hardware    Description
Type    Version      Version
----    ---------    ---------------    -----------
SP        11.14           11.x          SP version 11.14
SSP       11.14           12.x          SSP version 11.14
EIP       10.1             1.x          EIP version 10.1
TRIP      10.3             1.x          TRIP version 10.3
FIP       10.2             2.x          FIP version 10.2
HIP       10.2             1.x          HIP version 10.2
FSIP      182.3            1.x          FSIP version 182.3
MIP       11.4             1.x          MIP version 11.4
AIP       10.13            1.x          AIP version 10.13
FEIP      173.3            2.x          FEIP version 173.3

Microcode flash default images

Card    Microcode
Type    Version      device:filename
----    ---------    ------------------
CIP     22-8         slot0:cipp22-8     - Not present
```

Note The filenames of all CIP2 microcode images use the following nomenclature: cippnn-n, where *n* is the specific microcode version.

What Is the Cisco 7000 Series?

The Cisco 7000 series consists of the Cisco 7000 and Cisco 7010 routers.

Note For specific software and hardware requirements for the Cisco 7000 series systems, refer to the section “Software and Hardware Prerequisites” on page 13.

In the Cisco 7000, slot 5 is reserved for the RSP7000 (*7000 RSP* slot shown in Figure 8), which contains the system processor and performs packet switching functions; slot 6 is reserved for the RSP7000CI (*7000 CI* slot shown in Figure 8), which contains all of the environmental monitoring functions for the Cisco 7000. The remaining five slots (slots 0 through 4) are for interface processors, including the CIP2.

Figure 8 Cisco 7000 with RSP7000 and RSP7000CI Installed (Interface Processor End)

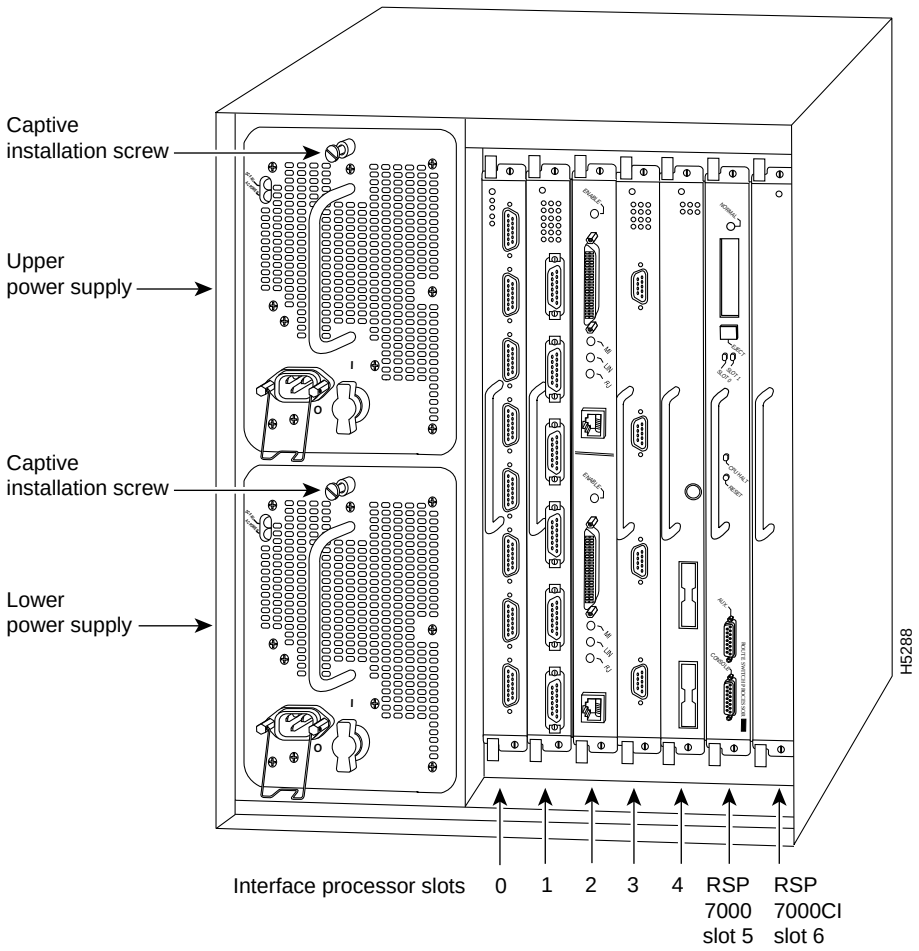
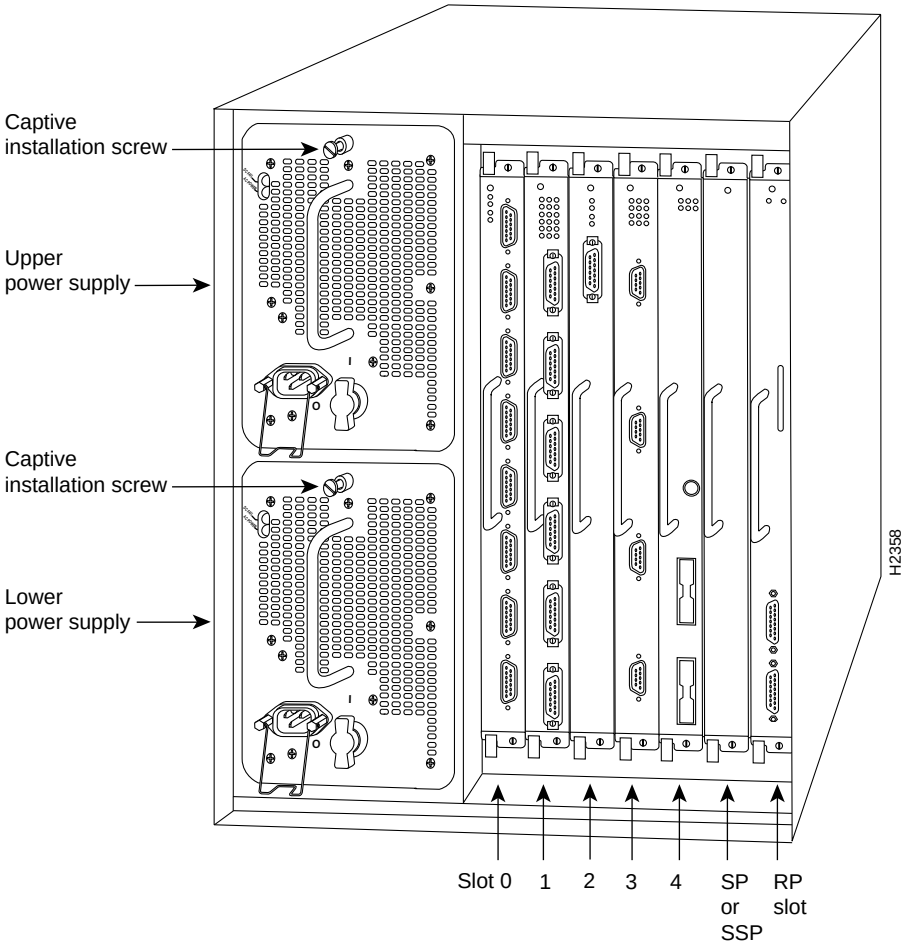


Figure 9 shows the interface processor end of the Cisco 7000, which provides access to the seven processor slots and the removable power supplies. When facing the interface processor end of the chassis, the SP (or SSP) and RP slots are on the far right. The five interface processor slots are numbered 0 to 4 from left to right and are reserved for interface processors, including the CIP2.

Figure 9 Cisco 7000 with RP and SP (or SSP) Installed (Interface Processor End)



In the Cisco 7010, slot 3 is reserved for the RSP7000 (*7000 RSP* slot shown in Figure 10), which contains the system processor and performs packet switching functions; slot 4 is reserved for the RSP7000CI (*7000 CI* slot shown in Figure 10), which contains all of the environmental monitoring functions for the Cisco 7010. The remaining three slots (slots 0 through 2) are for interface processors, including the CIP2.

Figure 10 Cisco 7010 with RSP7000 and RSP7000CI Installed (Interface Processor End)

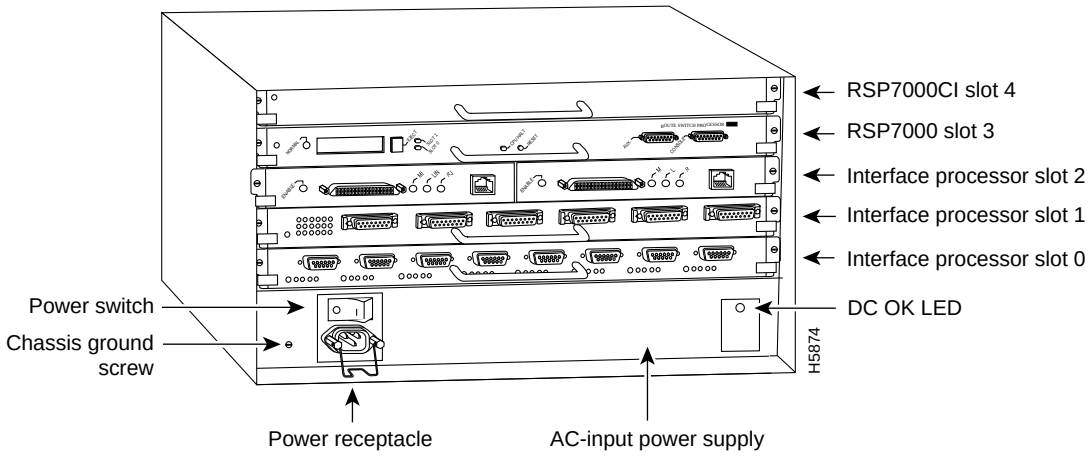
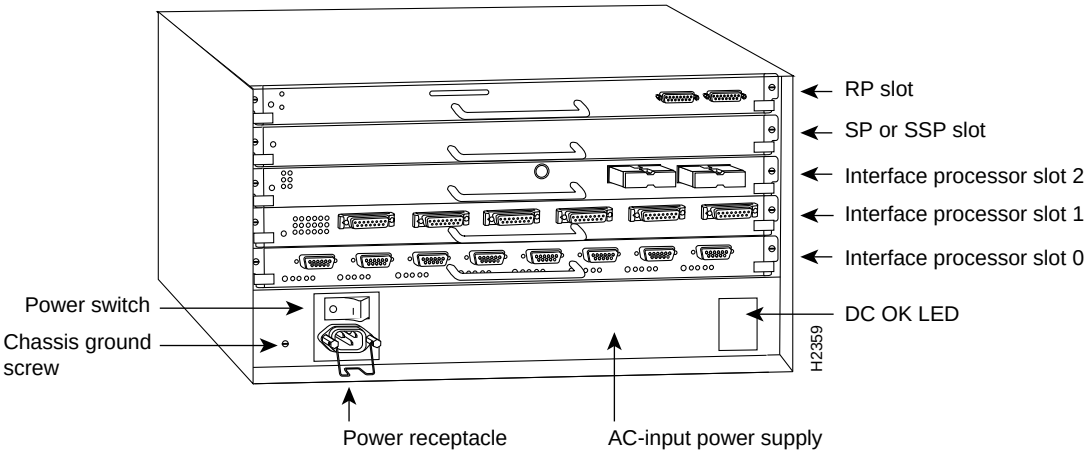


Figure 11 shows the interface processor end of the Cisco 7010, which provides access to the five processor slots. When facing the interface processor end of the chassis, the RP and SP (or SSP) slots are at the top. The three interface processor slots are numbered from the bottom up beginning with slot 0 (the bottom slot) through 2 (the center slot) and are reserved for interface processors, including the CIP2.

Figure 11 Cisco 7010 with RP and SP (or SSP) Installed (Interface Processor End)



What Is the Cisco 7500 Series?

The Cisco 7500 series consists of the Cisco 7505, Cisco 7507, and Cisco 7513 routers. The CIP2 will operate in the Cisco 7500 series routers.

Note For specific software and hardware requirements for the Cisco 7500 series systems, refer to the section “Software and Hardware Prerequisites” on page 13.

Network interfaces reside on modular interface processors, including the CIP2, which are inserted into interface processor slots and provide a direct connection between external networks and the high-speed CyBus in the Cisco 7500 series. Figure 12, Figure 13, and Figure 14 show the rear of the Cisco 7500 series routers: the five-slot Cisco 7505, the seven-slot Cisco 7507, and the thirteen-slot Cisco 7513, respectively.

In the Cisco 7505 (see Figure 12), one slot (4) is reserved for the Route Switch Processor (RSP1), which contains the system processor and performs packet switching functions. Slots 0 through 3 are for interface processors, including the CIP2.

Figure 12 Cisco 7505 (Interface Processor End)

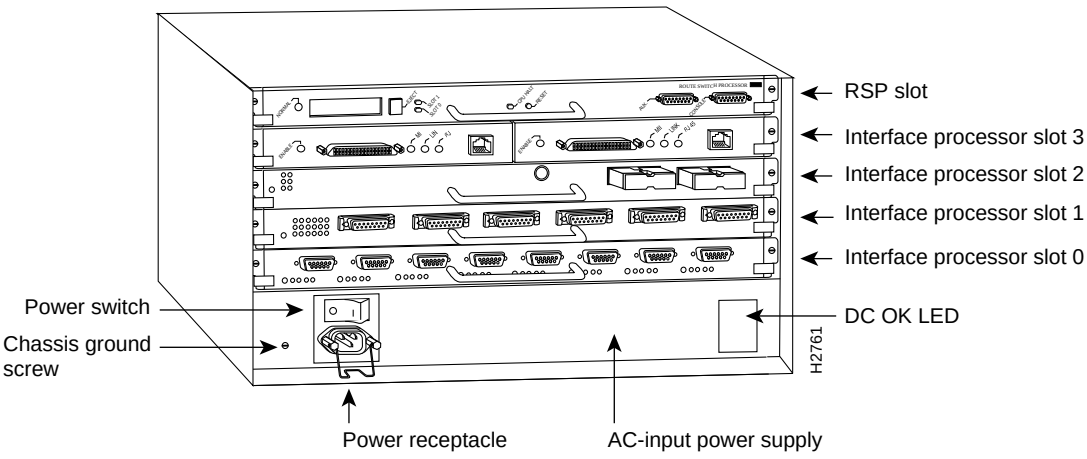


Figure 13 shows the rear of the Cisco 7507 router. In the Cisco 7507, up to two slots (2 and 3) are reserved for the Route Switch Processor (RSP2), which contains the system processor and performs packet switching functions. Slots 0 and 1 and 4 through 6 are for interface processors, including the CIP2.

Figure 13 Cisco 7507 (Interface Processor End)

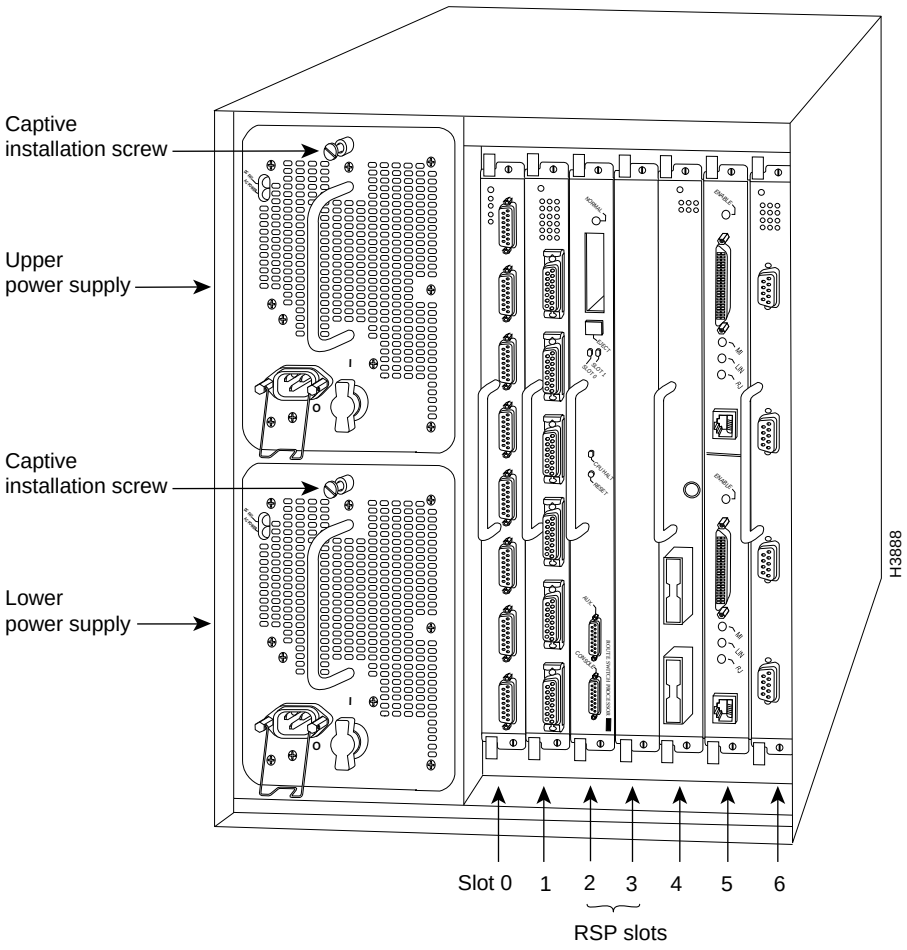
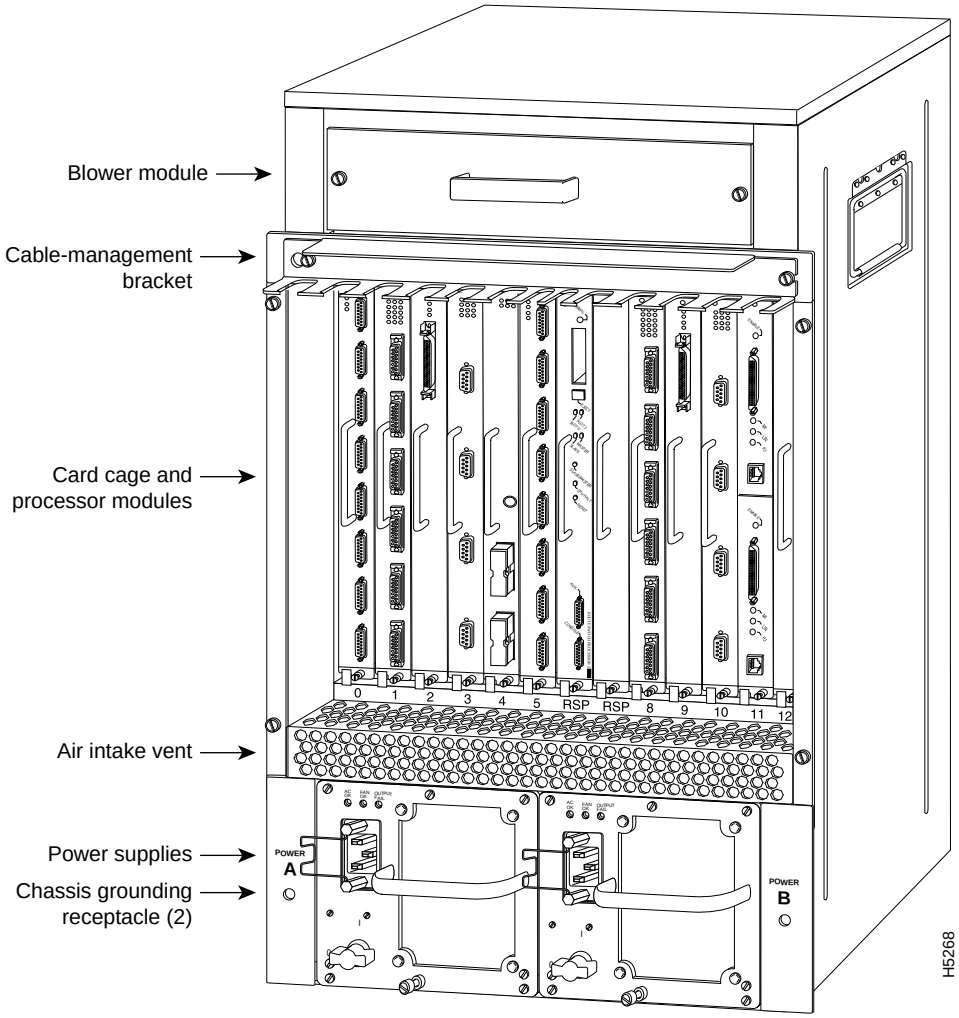


Figure 14 shows the rear of the Cisco 7513. Two slots (6 and 7) are reserved for the second generation Route Switch Processor (RSP2), which contains the system processor and performs packet switching functions. Slots 0 through 5 and 8 through 12 are for interface processors, including the CIP2.

Figure 14 Cisco 7513 (Interface Processor End)



Installation

The following sections provide a functional overview of online insertion and removal (OIR), and describe the procedures for installing or replacing CxBus interface processors in Cisco 7000 series routers. Before installing any new interfaces, ensure that your system meets the minimum software and microcode requirements described in the sections “Software and Hardware Prerequisites,” on page 13, and “Microcode Overview” on page 17.

The OIR feature allows you to remove and install a CIP2 without turning off system power. However, you must follow the insertion instructions carefully; for example, failure to use the ejector levers or insert the CIP2 properly can cause system error messages indicating a card failure.

Each unused interface processor slot contains an interface processor filler (which is an interface processor carrier without an interface card) to keep dust out of the chassis and to maintain proper airflow through the interface processor compartment. If you install a new CIP2, select an empty interface processor slot and remove the interface processor filler. If you replace a CIP2, *you can retain the existing interface configuration by removing the existing interface processor and installing the new one in the same slot*; however, the new CIP2 must be the same hardware type as the CIP2 you replaced.

Caution To avoid unnecessary errors, read the following OIR overview before removing or replacing a CIP2.

Following the OIR overview, proceed to the section “Removing a CIP2 or an Interface Processor Filler,” on page 26, for instructions on making an interface processor slot available for the new CIP2, then to the section “Installing a CIP2,” on page 29, for the installation instructions. After the new CIP2 is secure, follow the procedures in the section “Checking the Installation,” on page 35, to verify that it is installed and functioning properly.

Removing a CIP2 or an Interface Processor Filler

The CIP2 supports OIR, so you do not need to shut down the interface or the system power when you remove a CIP2; however, to prevent a possible interface control check on the mainframe, consult with your system administrator to take appropriate precautions. If you are installing a new CIP2, select an available slot and remove the interface processor filler. If you are replacing a CIP2, first remove the existing CIP2 and immediately place it component side up on an antistatic surface, then insert the new CIP2 in the same slot to retain the previous configuration for the new channel interface.

Figure 15 shows proper handling of an interface processor for installation in the Cisco 7010 or Cisco 7505 models. The processor slots are oriented horizontally in the Cisco 7010 and Cisco 7505, and vertically in the Cisco 7000, Cisco 7507, and Cisco 7513. When installing interface processors in these latter chassis, handle the interface processor in the same manner, but rotated 90 degrees clockwise.

Figure 15 Handling Interface Processors during Installation

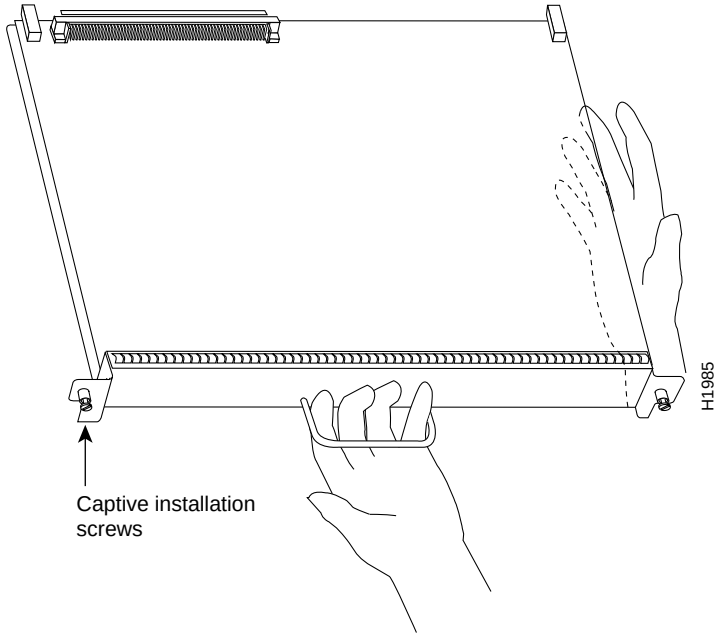
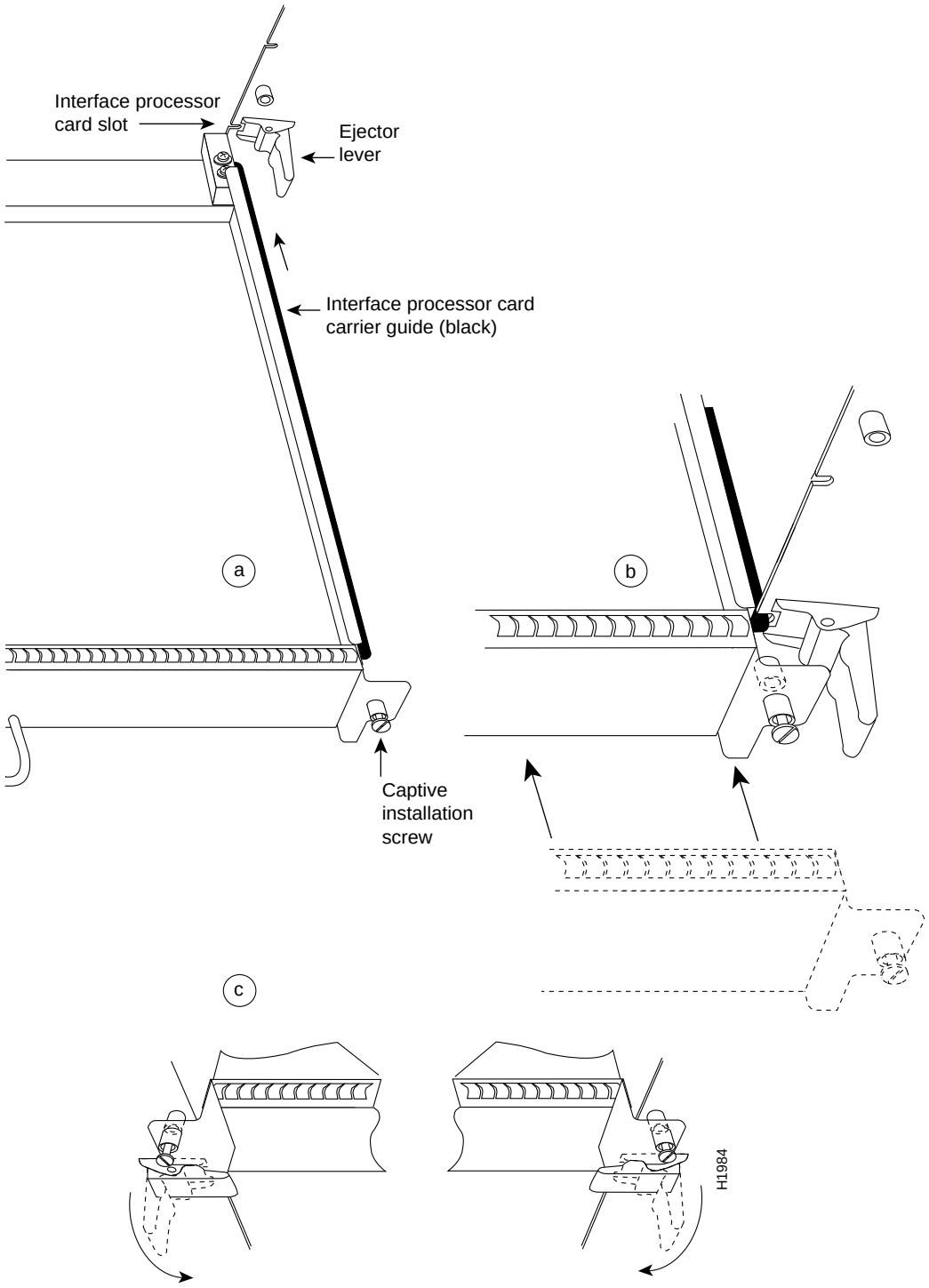


Figure 16 shows the functions of the ejector levers in the correct orientation for the horizontal processor slots in a Cisco 7010 and Cisco 7505 chassis. In a Cisco 7000, Cisco 7507, and Cisco 7513 chassis, the function of the ejector levers is the same, but the orientation is rotated 90 degrees clockwise for the vertical processor slots.

Figure 16 Function of the Ejector Levers



The function of the ejector levers (see Figure 16) is to align and seat the card connectors in the backplane. Failure to use the ejector levers and insert the interface processor properly can disrupt the order in which the pins make contact with the backplane.

Following are examples of *incorrect* insertion practices and their results:

- Using the handle to force the interface processor all the way into the slot can pop the ejector levers out of their springs. If you then try to use the ejector levers to seat the interface processor, the first layer of pins (which are already mated to the backplane) can disconnect and then remate with the backplane, which the system interprets as a card failure.
- Using the handle to force or slam the interface processor all the way into the slot can also damage the pins on the card connectors if they are not aligned properly with the backplane.
- When using the handle (rather than the ejector levers) to seat the interface processor in the backplane, you may need to pull the interface processor back out and push it in again to align it properly. Even if the connector pins are not damaged, the pins mating with and disconnecting from the backplane will cause the system to interpret a card failure. Using the ejector levers ensures that the card connector mates with the backplane in one continuous movement.
- Using only the handle to seat or remove an interface processor, or failing to push the ejector levers flat against the CIP2 faceplate, can leave some (not all) of the connector pins mated to the backplane, a state that will halt the system.

Using the ejector levers and making sure that they are pushed fully into position ensures that all three layers of pins are mated with (or free from) the backplane.

It is also important to use the ejector levers when you remove an interface processor to ensure that the card connector pins disconnect from the backplane in the logical sequence expected by the system. Any processor module that is only partially connected to the backplane can halt the bus. Detailed steps for correctly performing OIR are included with the following removal and installation procedures.

Refer to Figure 16 while performing the following steps to remove a CIP2 or interface processor filler. If you are removing an interface processor filler, proceed to Step 5. If you are replacing an existing CIP2, begin at Step 1. In the following procedures, two channel-related terms are used: *vary offline* refers to disabling an interface; *vary online* refers to enabling an interface. For instructions on how to vary the host channel or addresses online or offline, refer to the documentation for your operating system.

Step 1 Vary offline the addresses assigned to the PCA or ECA. For instructions on how to vary offline, refer to the documentation for your operating system.

Step 2 Use the **shutdown** interface command to shut down the router interface.

Step 3 On the PCA connector, place the select/bypass switch in bypass mode. (See Figure 6 on page 11.)

Step 4 Disconnect the interface cables from the CIP2 interface ports.

Step 5 Use a screwdriver to loosen both the captive installation screws on the CIP2 or interface processor filler. (See Figure 16a.)

Step 6 Place your thumbs on the ends of each of the ejector levers and simultaneously pull them both outward, away from the interface port (in the opposite direction from that shown in Figure 16c) to release the carrier from the slot. If you are removing a CIP2, this also releases the CIP2 bus connector from the backplane.

Step 7 Grasp the handle with one hand and pull the CIP2 or interface processor filler straight out of the slot, keeping your other hand under the carrier to guide it. (See Figure 15.) Keep the carrier parallel to the backplane. Avoid touching the card or any connector pins.

Step 8 Place the removed CIP2 on an antistatic mat or foam pad, or place it in an antistatic bag if you need to return it to the factory. If you removed an interface processor filler, store the filler in case you need it later to fill an empty slot.

Step 9 If the interface processor slot is to remain empty, install an interface processor filler to keep dust out of the chassis and to maintain proper airflow through the interface processor compartment.

This completes the removal procedure. Proceed to the next section to install a new CIP2.

Installing a CIP2

The CIP2 slides into any available interface processor slot and connects directly to the backplane of the Cisco 7000 series or Cisco 7500 series router. The backplane slots are keyed so that the CIP2 can be installed only in an interface processor slot. (Refer to Figure 8, Figure 10, Figure 12, Figure 13, or Figure 14, depending on your chassis type.) Figure 16 shows the functional details of inserting an interface processor and using the ejector levers. Figure 15 shows proper handling of an interface processor during installation.

Caution Remove or insert only one interface processor at a time. Allow at least 15 seconds for the system to complete the preceding tasks before removing or inserting another interface processor. Disrupting the sequence before the system has completed its verification can cause the system to assume that there has been a hardware failure.

Follow these steps to install a CIP2:

Step 1 Ensure that a console terminal is connected to the RP (or RSP) console port and that the console power switch is turned ON.

Step 2 Choose an available interface processor slot for the CIP2 and ensure that the interface cables are of sufficient length to connect the CIP2 to the channel.

Step 3 Hold the CIP2 handle with one hand, and place your other hand under the carrier to support the CIP2 (see Figure 15), and guide it into the slot. Avoid touching the card or any connector pins.

Step 4 Place the back of the CIP2 in the slot and align the notches along the edge of the carrier with the grooves in the slot. (See Figure 16a on page 27.)

Step 5 Keeping the carrier parallel to the backplane, carefully slide the CIP2 into the slot until the back of the faceplate makes contact with the ejector levers, then *stop*. (See Figure 16b on page 27.)

Caution Always use the ejector levers when installing or removing interface processor modules. A module that is partially seated in the backplane will cause the system to halt and subsequently crash, and shoving or slamming the interface processor into the slot can damage the backplane and connector pins.

Step 6 Using the thumb and forefinger of each hand to pinch each ejector lever, simultaneously push both ejector levers inward (toward the interface ports) until they snap into place and are parallel to the faceplate. (See Figure 16c on page 27.)

Step 7 Use a screwdriver to tighten the two captive screws on the interface processor faceplate. This prevents the interface processor from becoming partially dislodged from the backplane and ensures proper EMI shielding. (These screws must be tightened to meet EMI specifications.)

Proceed to the next section to attach the bus and tag and/or ESCON cables between the CIP2 interface ports and your channel.

Attaching the CIP2 to the Channel

The CIP2 can be connected to the channel using the bus and tag cables (for the PCA) and/or using a fiber-optic ESCON cable with duplex connectors (for the ECA). Bus and tag and ESCON connections each have their own special requirements. The following sections discuss bus and tag and ESCON connections.

Attaching the Bus and Tag Cables

The PCA is connected using the bus and tag cable with 78-pin connectors (the Y cable) and the bus and tag cables with 48-pin, type A connector blocks (the VA and VB cables). In general, a Y cable attaches to the PCA on the CIP2, and the VA and VB cables attach to the remaining ends of the Y cable.

Attaching the PCA to the Host Channel

Attach the PCA to the host as follows.

Caution To reduce the potential for problems, you should have an authorized service representative or other qualified service person perform the following procedure. To prevent hardware problems with your host processor, all the channel connections must be tight. A loose connection can cause the host processor or its channel to *halt*. All connections must be screwed together.

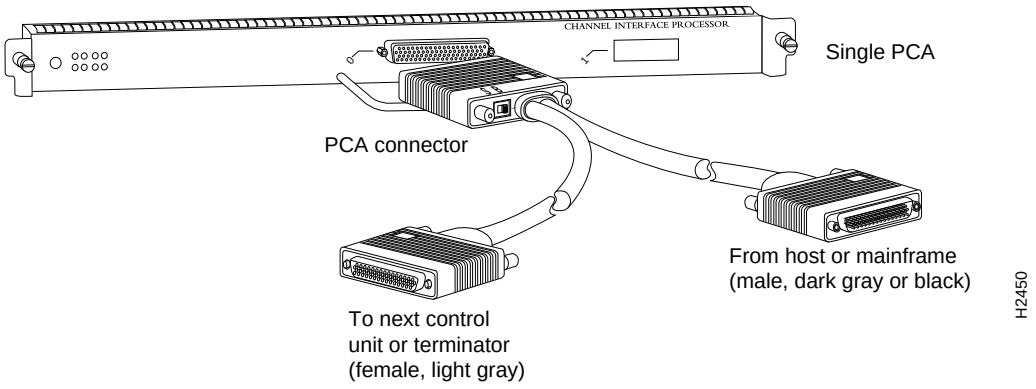
Step 1 Vary offline the host channel to which the PCA will be attached.

For instructions on how to vary the host channel offline, refer to the documentation for your operating system.

Caution If the select/bypass switch is in the select position when the PCA connector is detached, other devices on the channel and the mainframe operating system can be negatively affected.

Step 2 Attach the PCA connector of the Y cable to the PCA. (See Figure 17.)

Figure 17 Connecting or Removing the Y Cable



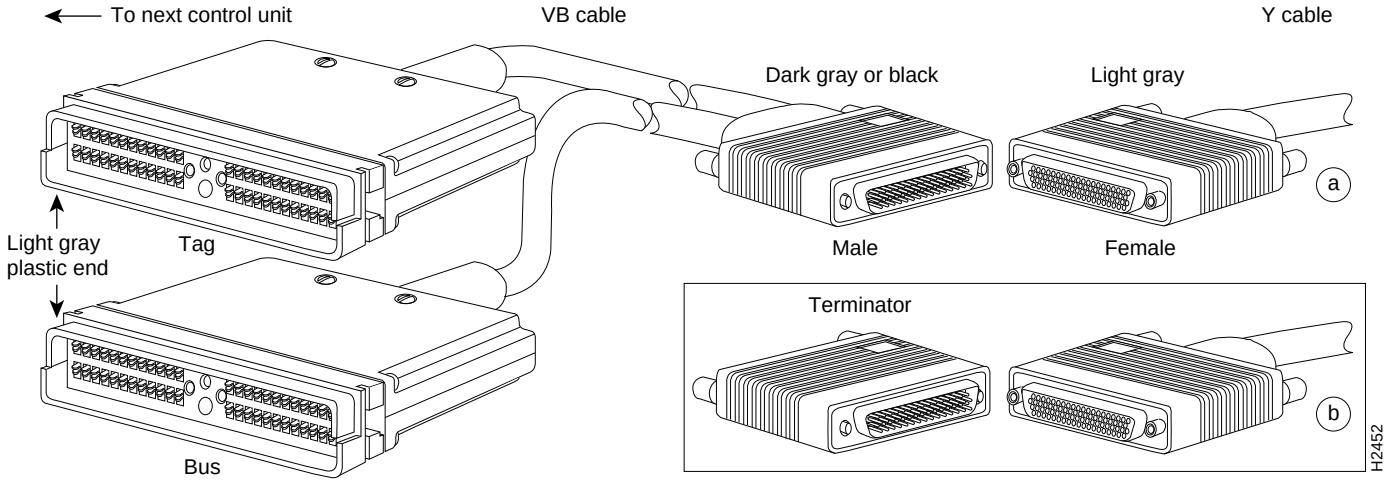
Step 3 Attach the female (light-gray) end of the Y cable (see Figure 18a) to the male (dark gray or black) end of the VB cable (that goes to the next control unit).

If the PCA is the *last* control unit on the channel, attach a terminator to the female end of the Y cable. (See Figure 18b.) *Do not attach a VB cable.*

Note If the PCA is the *last* control unit, channel termination is absolutely required to loop signals back to the host.

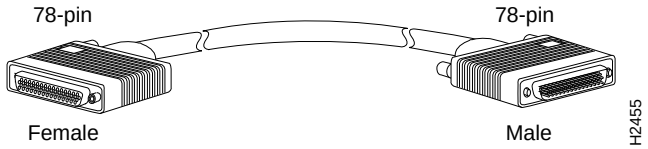
Caution To prevent potential system problems, do not connect the VB cable directly to the PCA. You must connect the Y cable to the PCA, then connect the VB cable to the Y cables as appropriate.

Figure 18 Connecting the VB Cable Between the Y Cable and the Next Control Unit



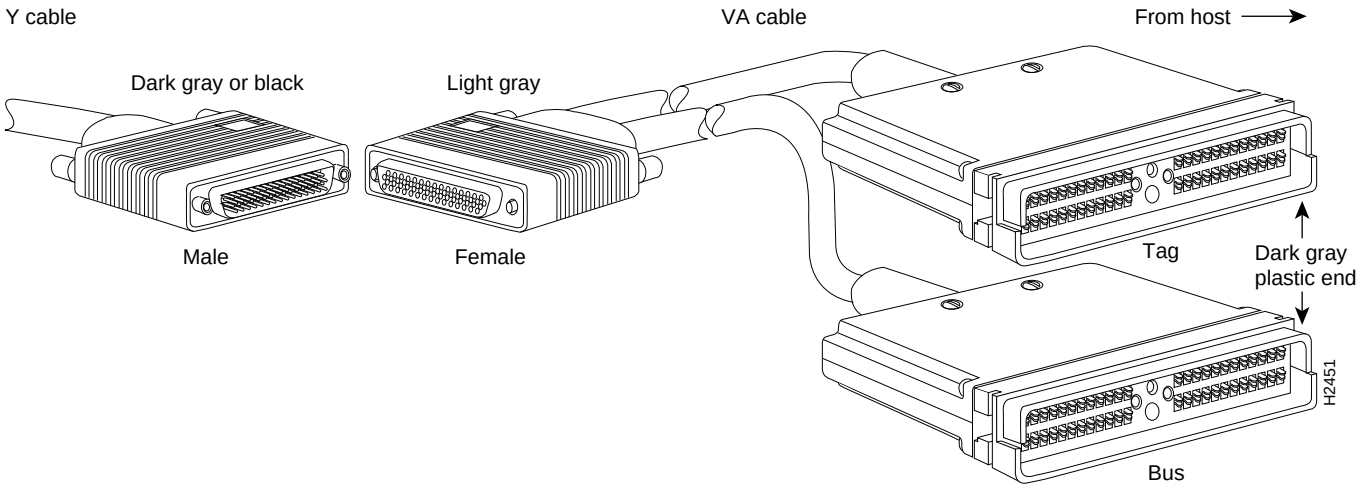
Step 4 If required, extend the length of the Y cable connections (between the VA and VB cables) with a straight-through cable (shown in Figure 19) that is available from IBM. This cable is not available from Cisco Systems.

Figure 19 Straight-Through Cable



Step 5 Attach the male (dark gray or black) end of the Y cable to the female (light gray) end of the VA cable that comes from the host. (See Figure 20.)

Figure 20 Connecting the VA Cable Between the Y Cable and the Host



Step 6 Leave the select/bypass switch (see Figure 6 on page 11) in bypass mode until the PCA connector is attached to the PCA.

Step 7 Connect the Y cable to the PCA.

Step 8 Place the select/bypass switch in select mode.

Step 9 Boot up the router.

Step 10 Configure the interface on the router.

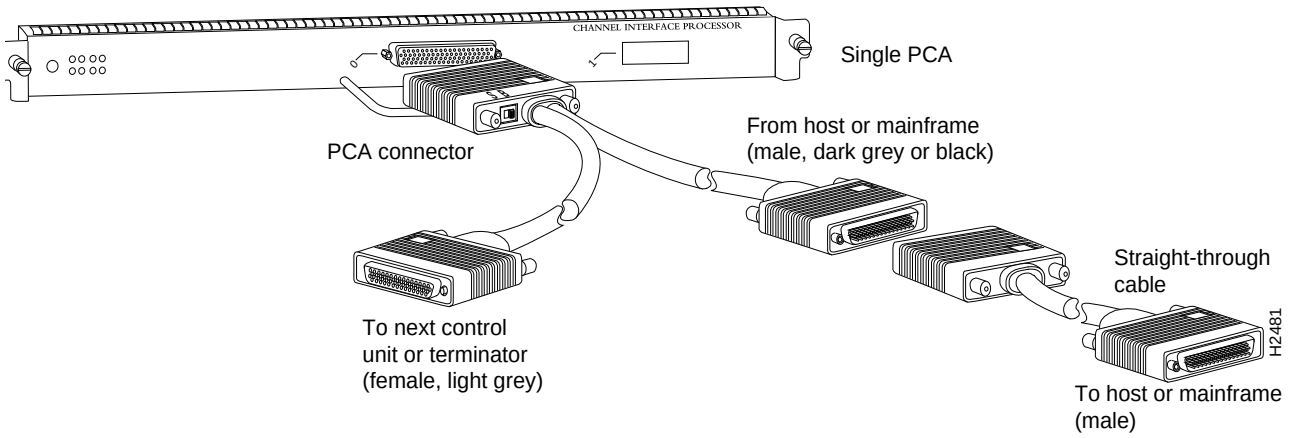
Step 11 Vary online the host channel.

For instructions on how to vary the host channel online, refer to the documentation for your operating system.

Step 12 It is also possible to connect the PCA to the host or mainframe using the straight-through cable (CAB-PCA-S) as shown in Figure 21.

This connection technique uses the Y cable and eliminates the requirement for the VA and VB cables from the host and to the next control unit, respectively. A straight-through cable can also be used from the Y cable to the next control unit; however, if no control unit exists, use a terminator.

Figure 21 Connecting the PCA and Host Using the Y Cable and Straight-Through Cable (CAB-PCA-S)



Caution To prevent damaging the PCA connector on the CIP2, by unintentionally disconnecting the Y cable from the PCA connector, make sure you provide adequate strain relief for the heavy bus and tag cables that attach to the PCA.

Detaching the Y Cable from the PCA

To properly detach a Y cable from the PCA, use the following procedure.

Caution To reduce the potential for problems, you should have an authorized service representative or other qualified service person perform the following procedure. To prevent hardware problems with your host processor, all the channel connections must be tight. A loose connection can cause the host processor or its channel to halt. Every cable must be tightly seated in its mating connector.

Step 1 Have the system operator vary offline all addresses assigned to the PCA. For instructions on how to vary addresses offline, refer to the documentation for your operating system.

Step 2 Place the select/bypass switch on the PCA connector in bypass mode. (See Figure 6 on page 11.)

To allow the propagation of channel signals to downstream control units while the PCA cable is disconnected, leave this switch in bypass mode.

Caution If the select/bypass switch is in select mode when the PCA connector is removed, other devices on the channel and the mainframe operating system might not operate properly.

Step 3 Remove the PCA cable connector (on the Y cable) from the PCA. (See Figure 17.)

Step 4 When you are finished with the task that required you to detach the PCA from the host channel, reattach the PCA connector (on the Y cable) to the PCA.

Step 5 Place the select/bypass switch on the PCA connector in select mode. (See Figure 6 on page 11.)

Step 6 Vary online all addresses assigned to the PCA. For instructions on how to vary addresses online, refer to the documentation for your operating system.

Caution To prevent damaging the PCA connector on the CIP2 by unintentionally disconnecting the Y cable from the PCA connector, provide adequate strain relief for the heavy bus and tag cables that attach to the PCA.

Attaching the ESCON Cable

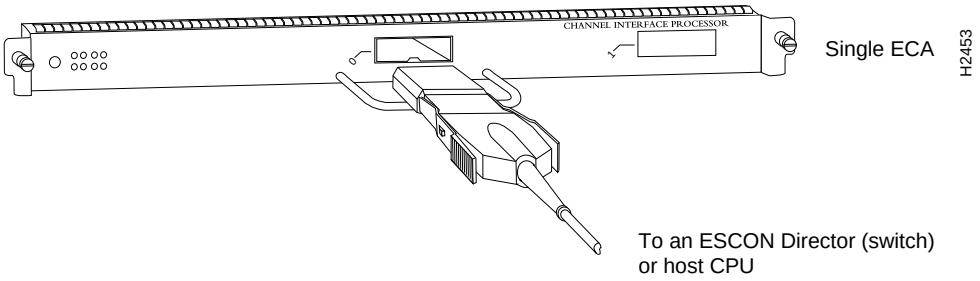
Following is the procedure for attaching the ESCON cable between the ECA and the host channel.

Caution To reduce the potential for problems, you should have an authorized service representative or other qualified service person perform the following procedure. To prevent hardware problems with your host processor, all the channel connections must be tight. A loose connection can cause the host processor or its channel to halt. Every cable must be tightly seated in its mating connector.

Step 1 Make certain the ECA interface is shut down (using the **shutdown** interface command) to prevent excessive error messages from being sent to the router log output. It is recommended, but not necessary, to vary offline the host channel to which the ECA will be attached. For instructions on how to vary the host channel offline, refer to the documentation for your operating system.

Step 2 Attach an ESCON cable between the ECA and the host channel. (See Figure 22.) Make certain the ESCON cable plug "clicks" into place in the receptacle on the ECA. If not, the connection will be incomplete and connection problems could result. It is best to visually inspect the connection after you make it, rather than relying on an audible cue in a noisy lab environment.

Figure 22 Connecting an ESCON Cable to the ECA



Step 3 Vary online the host channel. For instructions on how to vary the host channel online, refer to the documentation for your operating system.

Checking the Installation

After you install the CIP2 and cables, verify the installation by observing the LED states and the console display. When the system has reinitialized all interfaces, the enabled LED on the CIP2 (and on all interface processors) should go on. The console screen will also display a message as the system discovers each interface during its reinitialization. If you need to verify the operation of the interfaces, refer to the section “Running Diagnostic Tests” on page 44.

When you remove and replace interface processors, the system provides status messages on the console screen. These messages are for information only. The following sample display shows the events logged by the system as a CIP2 was removed from slot 1; the system then reinitialized the remaining interface processors and marked as *down* the CIP2 that was removed from slot 1. When the CIP2 was reinserted, the system marked the interface as *up* again because the interface was not shut down before the CIP2 was removed.

The sample display follows:

```
Router#
%OIR-6-REMCARD: Card removed from slot 1, interfaces disabled
%LINK-5-CHANGED: Interface CIP21/0, changed state to administratively down

Router#
%OIR-6-INSCARD: Card inserted in slot 1, interfaces administratively shut down
%LINK-5-CHANGED: Interface CIP21/0, changed state to up
```

When a new CIP2 is inserted or when a CIP2 is moved to a new slot, the system recognizes the new interface, but leaves it in a down state until you configure it and change the state to up with the **no shutdown** command.

The following sample display shows the events logged by the system as a new single-PCA CIP2 is inserted in slot 3:

```
Router#
%OIR-6-INSCARD: Card inserted in slot 3, interfaces administratively shut down
```

Verify that the CIP2 is installed correctly, as follows:

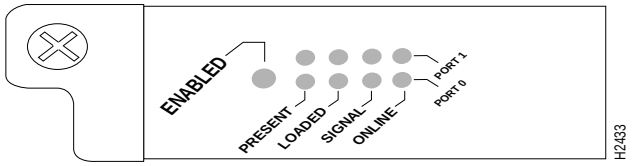
Step 1 While the system reinitializes each interface, observe the messages on the console display and verify that the system discovers the CIP2, as follows:

- If you installed a new CIP2, the system should recognize the new interface, but leave it configured as down.
- If you replaced a CIP2, the system should recognize the interface and place it in the same state (up or down) it was in before you removed the first CIP2.
- If the router fails to boot, displays an error message, or fails to recognize the CIP2, remove the CIP2 and reboot the router. If the router boots successfully, verify that the currently running system software and microcode meet the minimum requirements for CIP2 operation. (See the sections “Software and Hardware Prerequisites,” on page 13, and “Microcode Overview” on page 17.)

Step 2 When the ECA or PCA interface is up, check the activity of the interface with the CIP2 LEDs. Refer to the state descriptions in the section “CIP2 LED Indicators and Sequences” and Figure 3 on page 7. If no LEDs remain on, the CIP2 has not been successfully configured by the system and will not function, or the CIP2 is not inserted properly.

Step 3 When the reinitialization is complete, verify that the enabled LED on the CIP2 goes on and remains on. (See Figure 23.) If it does, proceed to Step 7. If it does not, proceed to the following step.

Figure 23 CIP2 LED Indicators



Step 4 If the enabled LED on the CIP2 fails to go on, the CIP2 card connector might not be fully seated in the backplane. Proceed as follows:

- Loosen the captive installation screws, then firmly push the ejector levers inward (toward the interface port) until both are parallel to the CIP2 faceplate.
- Tighten the captive installation screws.
- After the system reinitializes the interfaces, the enabled LED on the CIP2 should go on.

  If it does, proceed to Step 7. If it does not, proceed to Step 5.

Step 5 If the enabled LED still fails to go on, remove the CIP2 and try installing it in another available interface processor slot.

- If the enabled LED goes on when the CIP2 is installed in the new slot, there could be a failed backplane port in the original interface processor slot.
- If the enabled LED still fails to go on, but other LEDs on the CIP2 are on and indicate activity, the enabled LED on the CIP2 has probably failed. Proceed to Step 7 to resume the installation check.
- If the enabled LED still does not go on, *do not proceed with the installation.* Contact a service representative to report the faulty equipment and obtain further instructions. (Instructions for obtaining technical assistance are provided at the end of this document.)

Step 6 If the present LED fails to go on, the connection between the ECA or PCA and the motherboard might be faulty; however, *do not* attempt to disassemble the CIP2 in order to check this connection. Instead, contact a service representative.

Step 7 If the interface is new, refer to the publications listed in the section "If You Need More Information," on page 2, to configure the new interface. (This does not have to be done immediately, but an interface will not be available until you configure it.)

If this installation was a replacement CIP2, use the **show interfaces** or **show controllers cxbus** EXEC commands to verify the status of the interface. (For complete descriptions of the **show** commands, refer to the publications listed in the section "If You Need More Information," on page 2.)

If an error message is displayed on the console terminal, refer to the *System Error Messages* publication for error message definitions. If you experience other problems that you are unable to solve, contact a service representative for assistance.

This completes the CIP2 hardware installation.

CIP2 Microcode

The following sections discuss CIP2 microcode configuration requirements.

How Does CIP Microcode Ship?

For the Cisco 7000 series and Cisco 7500 series routers, CIP2 microcode is available on floppy diskettes, Flash memory cards (which also include the Cisco IOS release compatible with the microcode version), and via Customer Connection Online (CCO).

Starting with Cisco IOS Release 11.1, or later, CIP2 microcode images are shipped separately from the Cisco IOS software. For new Cisco 7000 series and Cisco 7500 series routers shipped with Cisco IOS Release 11.1, or later, the CIP2 microcode is shipped pre-installed on the Flash memory card.

For Cisco Release 11.1, or later, software upgrades, the CIP2 microcode is shipped or available on the following media:

- Via electronic download from CCO using File Transfer Protocol (FTP) for all 7000 family routers
- On a separate set of floppy diskettes shipped with Cisco IOS Release 11.1 diskettes for all Cisco 7000 series and Cisco 7500 series routers
- On floppy diskettes shipped with Cisco IOS Release 11.1 ROMs (RP-based Cisco 7000 series routers only)
- Preinstalled on a Flash memory card with Cisco IOS Release 11.1 (available as an upgrade for RP-based Cisco 7000 series routers only)

Note CIP2-compatible microcode images are bundled with all other Cisco IOS releases that support CIP2, including Cisco IOS Release 10.2(13), or later, Release 10.3(13), or later, and Release 11.0(10) or later.

CIP2 Microcode Upgrade Overview

Following is an overview of what you need to do to upgrade unbundled CIP2 microcode for the Cisco 7000 series and Cisco 7500 series routers.

Note In the following procedure, a CIP2-compatible Cisco IOS image *must* be booted *before* the CIP2 microcode image is copied to Flash memory.

For CIP2 microcode images that shipped on floppy diskettes or were obtained from CCO, do the following:

Step 1 Upload the CIP2 microcode image (and the Cisco IOS image if not on ROMs) on floppy diskettes or from CCO to a TFTP server.

Step 2 Remove any configuration commands that specify a CIP2 microcode image from the running configuration.

Step 3 Save your running configuration to a TFTP server or Flash memory.

Note If you have a Cisco 7000 series router and plan to install new software ROMs with Cisco IOS Release 11.1 or later, skip Steps 4 and 5 and turn off power to your router.

Install the new ROMs, then proceed to Step 6.

Step 4 Download the Cisco IOS image to Flash memory.

Step 5 Configure the router to boot from the Flash memory where the Cisco IOS image resides.

Step 6 Boot the Cisco IOS image.

Note The router must already be running a CIP2-compatible Cisco IOS image before performing a copy of the CIP2 microcode image to Flash memory in the following step, because the CIP2 microcode image must be "exploded" from the single image file on the TFTP server to multiple files in Flash memory. This capability is available in Cisco IOS Release 11.1 or later.

Step 7 Download the CIP2 microcode image to the Flash memory card in slot 0 or to flash memory, if you have a 7000 or 7010 with a RP.

Step 8 Restore the running configuration with the configuration you saved to the TFTP server in Step 3.

Step 9 Reconfigure the router, as required, to use the CIP2 microcode image stored in the Flash memory card in slot 0.

Step 10 Perform a microcode reload.

For CIP2 microcode that shipped on Flash memory cards, do the following:

Step 1 Insert the Flash memory card into a Flash memory card slot 0.

Step 2 Configure the router to boot from the Flash memory card in slot 0.

Note For the specific procedures associated with the steps in this overview, refer to the companion publication *Upgrading Software and Microcode in Cisco 7000 Family Routers* (Document Number 78-1144-xx), which includes the information and procedures necessary to upgrade your CIP2 microcode. The *Upgrading Software and Microcode in Cisco 7000 Family Routers* publication includes information on upgrading software and microcode images, transferring files to and from Trivial File Transfer Protocol (TFTP) servers, copying files between nonvolatile random-access memory (NVRAM) and Flash memory, and between TFTP servers and Flash memory; the publication also includes basic instructions for booting your system.

Configuring Microcode

This section describes how to modify the startup configuration to load different microcode images at startup, or to change existing configuration instructions and reenable the system default.

Important Note to Users If you received a preconfigured system with a CIP2 already installed, refer to Table 3 for the name of the CIP2 microcode image to specify when configuring your CIP2. Table 3 specifies the name of the minimum level of CIP2 microcode for a corresponding Cisco IOS release, which should be used if you are using a Cisco IOS release earlier than the Cisco IOS releases listed in the section "Software and Hardware Prerequisites," on page 13, or in the note on page 1.

Table 3 Cisco IOS Releases and CIP2 Microcode Images

Cisco IOS Release	CIP2 Microcode Image[1]
10.2	cipp20-8 or later
10.3	cipp20-8 or later
11.0	cipp21-8 or later
11.1	cipp22-6 or later

1. In general, CIP2 microcode image names that have the prefix "cipp" are compatible with the CIP2.

At system startup or reload, the system loads a microcode image for each processor type. All processors of the same type use the same microcode image; only one image for each type can load at startup. The CIP2 Flash memory provides a CIP2 microcode boot image. The entire CIP2 microcode image is located in a Flash memory card, on a floppy disk, or is available from CCO or from a TFTP server.

Whenever you upgrade software or microcode by downloading new images into Flash memory, you must configure the system to load the new image at startup. Otherwise, the system will continue to load the default image from the system, or attempt to load the previous image (if any) if it is still specified in the configuration file.

Note If you are running anything other than the default CIP2 microcode with your Cisco IOS image and you want to upgrade to a later version of Cisco IOS, and want to use the default CIP2 microcode that comes with that later version, you have to remove the **microcode cip flash** statement from the system configuration file, otherwise the Cisco IOS will try to load that old version of the CIP2 microcode.

To instruct the system to boot a CIP2 microcode image other than the default at startup, use the **microcode cip flash** [**bootflash** | **slot0** | **slot1**]:*filename* configuration command to add the instructions to the configuration file.

Follow these steps to configure the microcode for a CIP2 on a router configured with Cisco IOS Release 11.1(5) or later.

Note If you are currently running a previous Cisco IOS release, refer to the appropriate configuration and command reference publications for specific commands that apply to this procedure depending on your Cisco IOS release. All Cisco IOS release documentation is available on the Cisco Connection Documentation, Enterprise Series CD-ROM.

If you plan to load a microcode image from an individual file or a bundled system image stored in Flash memory, enter the **show flash slot 0:** EXEC command to display the contents and verify the exact name of the file (*cip1234* is used in this example):

```
Router> show flash slot0:

(additional displayed text omitted)

-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. FFFFFFFF A831B720 3828CC  16   3549260  Feb 24 1996 20:28:56 rsp-k-mz.111-5
2   .. FFFFFFFF 83A6447F 8B8D18  16   761932   Apr 17 1996 15:15:59 cip1234

(additional displayed text omitted)

5419388 bytes available (15158916 bytes used)
```

Step 1 Enter the privileged EXEC mode command interpreter, as follows:

```
Router> enable
Password:
Router#
```

Note For complete information on the command interpreter and software functions, refer to the publications listed in the section “If You Need More Information” on page 2.

Step 2 If you need to copy a new CIP2 microcode image into your system’s Flash memory, refer to the section “Using Flash Memory,” on page 41, then proceed to Step 3.

Step 3 In privileged command mode, enter router configuration mode and specify that the console terminal will be the source of the configuration subcommands, as follows:

```
Router# configure terminal
```

To load the microcode from an individual microcode image that is stored as a file in Flash memory, enter the **microcode** command, the processor type, the specific memory location of the CIP2 microcode image, and the exact argument for *filename* (*cip1234* is used in this example):

```
Router(config)# microcode cip flash slot0:cip1234
```

The **no microcode** command cancels any existing instructions to load an image from Flash memory:

```
Router(config)# no microcode cip flash slot0:cip1234
```

Step 4 To save the configuration file, press **Ctrl-Z**, then copy the new configuration to nonvolatile random-access memory (NVRAM) as follows:

```
Router# copy running-config startup-config
```

The **microcode reload** command must invoked whenever you modify the system default to load a microcode image, using the **microcode cip flash** command.

Step 5 To verify that the correct microcode is loaded according to the new instructions, enter the **show controller cbus** EXEC command. The resulting display indicates the currently loaded and running microcode version for each interface processor.

Step 6 To verify the contents of the configuration file, enter the **show running-config** and **show startup-config** EXEC commands. You can also verify that the correct system image is configured to load at system restart or reload.

This completes the procedure for configuring microcode. For complete descriptions of the **show** commands, refer to the publications listed in the section “If You Need More Information” on page 2.

Using Flash Memory

The following sections discuss various Flash-memory functionality that you might need.

Copying to Flash Memory on an RSP or RSP7000

Copying a new image to Flash memory might be required whenever a new microcode image becomes available. Use the command **copy tftp:***filename* [**bootflash** | **slot0** | **slot1**]:*filename* for the copy procedure where **tftp:***filename* is the source of the file and [**bootflash** | **slot0** | **slot1**]:*filename* is the destination in onboard Flash memory or on either of the Flash memory cards.

An example of the **copy tftp:***filename* command for Cisco IOS Release 11.1 follows:

```
Router# copy tftp:cip1234 slot0:cip1234
2283972 bytes available on device flash, proceed? [confirm]
Address or name of remote host [hamachi.cisco.com]?
Accessing file "cip1234" on hamachi.cisco.com ...FOUND
Loading mhoerler/cip1234 from 1.1.1.22 (via Ethernet0/0): !Verifying via checksum...

Flash verification successful.  Length = 1, checksum = 0xFFFF

--- expanding multi-segment file ---
flash:cip1234_kernel_hw4 size = 238626
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Verifying via checksum...
vvvvvvvvvvvvv
```

```
Flash verification successful.  Length = 238626, checksum = 0x0000

--- expanding multi-segment file ---
flash:cip1234_seg_802 size = 198600
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Verifying via checksum...
vvvvvvvvvvvv

Flash verification successful.  Length = 198600, checksum = 0x9237

--- expanding multi-segment file ---
flash:cip1234_seg_csna size = 102392
!!!!!!!!!!!!!!!!!!!!Verifying via checksum...
vvvvvv

Flash verification successful.  Length = 102392, checksum = 0x771E

--- expanding multi-segment file ---
flash:cip1234_seg_eca size = 461408
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!Verifying via checksum...
vvvvvvvvvvvvvvvvvvvvvvvvvvvv

Flash verification successful.  Length = 461408, checksum = 0xB791

--- expanding multi-segment file ---
flash:cip1234_seg_offload size = 52608
!!!!!!!!!!Verifying via checksum...
vvv

Flash verification successful.  Length = 52608, checksum = 0x0FBC

--- expanding multi-segment file ---
flash:cip1234_seg_pca size = 69360
!!!!!!!!!!!!!!Verifying via checksum...
vvvv

Flash verification successful.  Length = 69360, checksum = 0x737F

--- expanding multi-segment file ---
flash:cip1234_seg_tcpip size = 175320
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Verifying via checksum...
vvvvvvvvvv

Flash verification successful.  Length = 175320, checksum = 0xD416
```

Note In the preceding example, the exclamation points (!!!) appear as the file is downloaded, and the “C” characters signify calculation of the checksum, which is a verification that the file has been correctly downloaded to the Flash memory card.

Additional Flash Memory Commands

Following are additional commands related to the Flash memory in the single in-line memory module (SIMM) on the RSP1, RSP2 and RSP7000 (called *bootflash*) and in PCMCIA Flash memory cards. (The following example assumes you are currently accessing the Flash memory card in PCMCIA slot 0.) You can determine which PCMCIA slot you are accessing using the **pwd** command as follows:

```
Router# pwd
slot0
```

You can move between Flash memory media using the **cd** [**bootflash** | **slot0** | **slot1**] command as follows:

```
Router# cd slot0
slot0
Router# cd slot1
Router# pwd
slot1
```

You can list the directory of any Flash memory media using the **dir** [**bootflash** | **slot0** | **slot1**] command as follows:

```
Router# dir
-#- -length- -----date/time------ name
1   4601977  May 19 1994 09:42:19 myfile1
6   679      May 19 1994 05:43:56 todays–config
7   1        May 19 1994 09:54:53 fun1
```

You can delete a file from any Flash memory media using the **delete** command as follows:

```
Router# delete slot0:fun1
Router# dir
-#- -length- -----date/time------ name
1   4601977  May 19 1994 09:42:19 myfile1
6   679      May 19 1994 05:43:56 todays–config
```

To verify that the **delete** command was successful, use the **dir/all/long** command.

Note Files that are deleted are simply marked as deleted, but still occupy space in Flash memory. To remove them, use the **squeeze** command.

The **squeeze** command permanently removes files, which are marked as deleted, and pushes all other undeleted files together to eliminate spaces between them.

Following is the syntax of the squeeze command:

```
Router# squeeze slot0:
All deleted files will be removed, proceed? [confirm]
Squeeze operation may take a while, proceed? [confirm]
ebESZ
```

To prevent loss of data due to sudden power loss, the “squeezed” data is temporarily saved to another location of Flash memory, which is specially used by the system.

In the preceding command display output, the character “e” means this special location has been erased (which must be performed before any write operation). The character “b” means that the data that is about to be written to this special location has been temporarily copied. The character “E” signifies that the sector which was temporarily occupied by the data has been erased. The character “S” signifies that the data was written to its permanent location in Flash memory.

The **squeeze** command operation keeps a log of which of these functions has been performed so upon sudden power failure, it can come back to the right place and continue with the process. The character “Z” means this log was erased after the successful **squeeze** command operation.

Recovering from Locked Blocks

A locked block of Flash memory occurs when power is lost or a Flash memory card is unplugged during a write or erase operation. When a block of Flash memory is locked, it cannot be written to or erased, and the operation will consistently fail at a particular block location. The only way to recover from locked blocks is by reformatting the Flash memory card with the **format** command.

Caution Formatting a Flash memory card to recover from locked blocks will cause existing data to be lost.

Running Diagnostic Tests

There are six PCA and ECA diagnostic test routines, as follows:

- Processor test 1
- Processor test 2
- I/O device tests
- Serial link controller (SLC) device tests
- Internal electrical wrap
- External optical wrap (ECA only) or external electrical wrap (PCA only)

  The external wrap routine will run in two modes: optical and electrical.

Note All diagnostic tests are run every time the adapter is started. They cannot be run independently. The wrap tests require special wrap plugs for the PCA and ECA; contact a service representative to obtain the appropriate wrap plugs.

The interface has to pass the first five tests. The sixth test (which is the same as the fifth, but with a different mode for the optical wrap plug for the ECA, instead of electrically wrapping the interface) will fail if no wrap plug is installed or if the interface is connected to the channel. This type of failure will not affect the channel.

If a wrap plug is inserted, following is how the wrap diagnostics will be repeated:

- Until a failure occurs
- Until the wrap plug is removed (which may be reported as a failure depending on when you pull the wrap plug)
- Until you enable the second adapter (as in a dual channel-attached CIP2)

If you suspect that an adapter might be the cause of a problem you are seeing, you can run a single pass of the diagnostic tests on an installed PCA or ECA interface by entering configuration mode and specifying that the console terminal will be the source of the configuration subcommands, as follows:

```
Router# configure terminal
```

Next, specify the slot/port number (interface processor slot number/port number) of the interface for which you want the diagnostic tests to run by entering the **interface channel** command followed by the slot/port of the interface.

The example that follows is for a CIP2 interface in interface processor slot 1:

```
Router(config)# interface channel 1/0
```

To run the diagnostic tests once, enter the **shutdown** command and then the **no shutdown** command, as follows:

```
Router(config)# shutdown
Router(config)# no shutdown
Ctrl-Z
Router#
```

The **no shutdown** command causes the diagnostic tests to run on the PCA or ECA interface you selected. If no failures occur, you can rule out that adapter as the source of your problem.

Markus Hoerler and Tim Masterson need to review this for new ESCON diagnostics.

URL to this doc: http://wwwin-itg/ccden2/data/doc/hardware/fusion/7000/cfig_nts/3335cip2.htm

Also several new Cisco IOS releases will be required to support the new ESCON adapter.

Also, new CIP2 uCode release will be required for new ESCON adapter.

Cisco Connection Online

Cisco Connection Online (CCO), formerly Cisco Information Online (CIO), is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional content and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously—a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, Internet e-mail, and fax download options, and is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com.
- Telnet: `cco.cisco.com`.
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and baud rates up to 14.4 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact `cco-help@cisco.com`. For additional information, contact `cco-team@cisco.com`.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or `tac@cisco.com`. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or `cs-rep@cisco.com`.

This document is to be used in conjunction with the *Cisco 7000 Hardware Installation and Maintenance*, *Cisco 7010 Hardware Installation and Maintenance*, *Cisco 7505 Hardware Installation and Maintenance*, *Cisco 7507 Hardware Installation and Maintenance*, *Cisco 7513 Hardware Installation and Maintenance*, and *Channel Interface Processor Microcode Release Note and Microcode Upgrade Requirements* publications. (3335cip2.fm)